A Secure Decentralized Event-Triggered Cooperative Localization in Multi-Robot Systems Under Cyber Attack

TOHID KARGAR TASOOJI AND HORACIO J. MARQUEZ, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada
Corresponding author: Tohid Kargar Tasooji (kargarta@ualberta.ca)

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

ABSTRACT We study the problem of secure decentralized event-triggered cooperative localization (SDECL) for a team of mobile robots in an adversarial environment, where the objective is to perform localization in the presence of a malicious attacker. We consider a scenario in which an intruder is able to attack the communication channels between exteroceptive sensors and filter of the robot and between two robots independently. First, we design a secure decentralized event-triggered cooperative localization in the multi-robot system against random Denial of Service (DoS) and False Data Injection (FDI) attacks. Then, we provide sufficient conditions that ensure the resilience and convergence of the proposed algorithm when the attacker signal rate is bounded. Simulation results show that by properly tuning the parameters of the event-triggered mechanism and considering bounded attack rate, the proposed algorithm is resilient against cyber attacks. Also, experimental results using four e-puck2 mobile robots have demonstrated the effectiveness of the proposed method.

INDEX TERMS Event-triggered mechanism, multi-robot system, cooperative localization, malicious attacker.

I. INTRODUCTION
In recent years, mobile robots have been widely utilized in the solution of multiple tasks, including surveillance, rural search, and exploration. Accurate and reliable sensors and communication devices have made it possible to consider multi-robot systems in which a team of robots work cooperatively to complete certain task [1]. In this context, precise localization of each robot in the group is crucial for a successful operation. However, precise localization highly depends on reliable sensor measurements which is typically unavailable in practical applications. One solution to this problem is to employ cooperative localization (CL), an area that has attracted much researcher [2], [3], [4], [5]. The basic CL problem consists of enabling each robot to estimate its position by sensing and communicating with the rest of the robots in the team. As a result, communication and exchange of information between robots is a critical factor in CL [6]. Despite significant advances in the development of reliable sensor and communication devices, sensor measurements and communication networks can be maliciously compromised [9]. An attacker can hijack the communication channels between the exteroceptive sensors and the robot’s filter, or between filters, and then block or modify the communication data shared between system components, thus degrading localization quality.

In general, cyber attacks can be mainly classified as either denial of service (DoS) or false data injection (FDI) attacks. In DoS attacks, the attacker interrupts the transmission of data through the communication network by propagating a random jamming signal. In FDI attacks, on the other hand, the attacker can affect the trustworthiness of data by manipulating the transmitted data over the network. Zhu et al. [17] address the adaptive torus-event-based control problem for a class of networked Takagi-Sugeno (T-S) fuzzy systems under deception attacks. Pan et al. [18] investigate the
$L_2 - L_\infty/H_\infty$ optimization control problem for a family of nonlinear plants by Takagi–Sugeno (T–S) fuzzy approach with actuator failure. Pan et al. [19] study the problem of resilient event-triggered (RET)-based security controller design for nonlinear NCSs described by interval type-2 (IT2) fuzzy models subject to nonperiodic DoS attacks. Mo et al. [10], Fawzi et al. [11], Shoukry et al. [12], Li et al. [13], Zhang et al. [14], Su et al. [15], and Lin et al. [21] among others, have investigated the problem of secure state estimation for networked control system (NCS) against cyber attacks. To the best of our knowledge, however, there are few works addressing secure state estimation for multi-agent systems (MASs) under cyber attacks [22], [23], [24], [25], [26], [27], [28], [29].

The use of a network is instrumental in establishing communication between robots. As the number of sensors, actuators and robots increase, however, the amount of information packets that needs to be transferred between robots can increase significantly. This increase brings two problems that need attention during the design, namely; bandwidth usage and electric power consumed during transmission. Power consumed during transmission can be critical when working with mobile robots that operate with limited energy resources. Bandwidth constraints, on the other hand, may bring undesirable effects such as communication delays and packet losses in the communication between agents [34]. Both these issues can be alleviated by reducing the amount of information exchanged between system components. Event-triggered systems have emerged as an alternative to classical periodic sampling systems that can produce similar results while reducing communication between components. The main idea behind an event-triggered mechanism (ETM) is that transfer of information takes place only when needed, according to a decision made by a triggering condition [7], [8]. Event-triggered control problems have been extensively studied, however event-triggered cooperative localization has received comparatively much less attention. See references [30], [34], [35]. In general, event-triggered systems can offer excellent performance while reducing communication and energy consumption. The reduction in information transfer, however, can make event-triggered systems more vulnerable against random delays, packet dropout and cyber attacks, compared to time-triggered systems.

A. RELATED PAPERS ON SECURE STATE ESTIMATION AGAINST CYBER ATTACKS

Most of the literature on the subject considers the problem of secure state estimation against cyber attacks for single agent systems. Mo et al. [10] consider the problem of secure state estimation against integrity attacks (or FDI attacks) where the attacker intentionally manipulates the sensor measurements. Fawzi et al. [11] study the problem of secure estimation and control for linear systems where the attacker hijacks the sensor measurements and actuators. The authors design a resilient state estimator and state-feedback controller such that the state of a system is recovered accurately and improve the system resilience against deception attacks. Shoukry et al. [12] consider a state reconstruction for discrete-time linear systems under sparse sensor attacks/noise. Li et al. [13] study the problem of remote state estimation where a malicious attacker launches a jamming signal on the communication channel between the sensor and remote estimator. Zhang et al. [14] propose an optimal DoS attack scheduling strategy where the attacker decides when or where to attack the communication channel in order to degrade the performance of the remote estimator. Su et al. [15] investigates malicious attack detection and secure state estimation for CPSs with sensor attacks. Lin et al. [21] derive an optimal estimator for CPSs whose communication channels are subject to mixed DoS and FDI attacks. Qu et al. [16] investigate the chance-constrained $H_\infty$ state estimation problem for a class of time-varying neural networks subject to measurements degradation and randomly occurring deception attacks.

Unlike [10], [11], [12], [13], [14], [15] and [21] that focus on single agent systems, some related works consider secure state estimation for MASs. Liu et al. [22] studies event-triggered distributed state estimation for discrete-time linear systems with multiple communication channels under DoS attacks. Using the covariance intersection fusion framework, the authors design distributed Kalman filters resilient against DoS attacks. Liu et al. [23] further extend the results for nonlinear systems and design resilient event-triggered distributed state estimation filters against DoS attacks where the attack duration is bounded. Chen et al. [24] address the distributed resilient filtering problem for power systems against DoS attack. Chen et al. [25] consider a saturated innovation update mechanism for resilient distributed state estimators against sensor attacks. An et al. [26] study the problem of distributed secure state estimation for discrete-time linear systems under sparse sensor attacks. The authors also implement the proposed algorithm over a multi-agent network. Lu et al. [27] investigate secure state estimation of MASs with both faulty and malicious agents.

Different from [22], [23], [24], [25], [26], and [27] where each agent reconstruct the states without cooperation in the presence of attacks, few works consider the secure cooperative state estimation under malicious attacker. Su et al. [28] consider resilient cooperative state estimation in unreliable multi-agent networks. A gradient descent scheme is adopted for each agent based on local measurements. In this approach, each agent transmit its updates to the other agents in the neighbourhood. Lu et al. [29] address distributed secure state estimation where a group of agents estimate the states cooperatively under malicious attacks. A distributed switched gradient descent scheme is adopted to reconstruct the states in the presence of malicious nodes.

B. RELATED PAPERS ON ATTACK DETECTION

To mitigate the effects of attack and improve resilience, several attack detection methods have been proposed in the literature. Huang et al. [37] investigate a defense mechanism
for distributed consensus estimator using the measurement of the on-board sensors for each node to detect the false data injection attack. Li et al. [43] design the secured distributed state estimator by adding an attack detector, when the set of attacked sensors is known to be time invariant. Manandhar et al. [36] design a framework for the smart-grid system using the KF estimator together with the \( \chi^2 \)-detector and Euclidean detector. The authors show that the \( \chi^2 \)-detector has better performance in detecting different types of faults and attacks, such as DoS attacks and random attacks on the system.

### C. RELATED PAPERS ON DECENTRALIZED EVENT-TRIGGERED COOPERATIVE LOCALIZATION IN MULTI-ROBOT SYSTEMS

The event-triggered cooperative localization problem for multi-robot systems has received some attention. Ouimet et al. [30] propose a decentralized event-triggered cooperative localization (DECL) algorithm for a group of mobile robots where the objective is to perform localization with limited communication resources, and study the effect. Reference [35] extends the results and consider the effect of random delays in the event-triggered cooperative localization.

### D. MAIN CONTRIBUTION

Compared to the existing literature on cooperative localization [2], [3], [4], [5], [6] and our previous works on decentralized event-triggered cooperative localization [34], [35], this paper investigates secure decentralized event-triggered cooperative localization for multi-robot systems operating with an unreliable communication network subject to DoS and FDI attacks. Also, we consider a scenario in which each robot can sense and communicate with other robots simultaneously within certain range, extending the results of our previous works [34], [35]. Contrary to the case of secure state estimation against a single type of attack (either DoS or FDI) for a single agent system as in references [10], [11], [12], [13], [14], [15], we consider secure state estimation for MASs in the presence of mixed DoS and FDI attacks. Different from [22], [23], [24], [25], [26], and [27] where agents reconstruct states without cooperation, we design a resilient state estimation scheme in which agents reconstruct the states cooperatively in the presence of mixed attacks.

In contrast to [24], [25], [26], [27], [28], and [29] that employ periodic sampling, our solution relies in a mixed-type event-triggered mechanism which significantly reduces the average transmission of information through the network. Moreover, our approach to secure communication is different from [22], [24], [26], [27], and [39]. In our approach we consider a detector for each robot based on received innovations to decide whether the measurements received have been attacked or not. Also, the majority of the literature on secure state estimation uses simulations to justify the proposed solution. In this work we tackle the actual implementation of our solution using a group of mobile robots. The implementation is not trivial and bring up multiple challenges.

To the best of our knowledge, the problem of event-triggered cooperative localization has not been investigated for multi-robot systems in the presence of cyber attacks. Departing from our previous work in references [34] and [35], we modify our DECL algorithm to account for the effect of cyber attacks. Our work involves both theoretical development of the solution and practical implementation using a fleet of e-puck2 robots. The experimental results are expected to provide a preliminary effort towards bridging the gap between theoretical analysis and experimental validation. The main challenges involved in this work include (1) designing a secure CL algorithm against cyber attacks that guarantees satisfactory localization performance while maintaining a low communication volume between system components, and (2) implementing the solution using a multi-robot hardware platform and verify the effectiveness of the algorithm.

Our main contribution can be summarized as follows: First, we introduce a SDECL algorithm for a group of mobile robots explicitly focusing on the problem of cyber attacks. We consider a scenario in which the adversary is able to attack the communication channels between the exteroceptive sensors and the robot’s filter and between two robots independently. Second, we prove the effectiveness of the proposed algorithm by computing the stochastic boundedness of the estimation error in mean square for the SDECL algorithm under cyber attacks. We provide sufficient conditions that ensure the resiliency and convergence of proposed algorithm when the attacker signal is bounded. We show that by choosing a proper event-triggered condition, the estimation error and covariance of the state estimator remain bounded while reducing the data transmission between the sensor and the filter. Third, when the attack signals are unbounded we introduce an attack detection mechanism capable of detecting the presence of an attack. Finally, comparative experiments are carried out using a team of four e-puck2 robots to validate the corresponding theoretical results. The experimental results show the effectiveness and robustness of SDECL algorithm in the presence of cyber attacks.

The rest of this paper is organized as follows. Section II contains the dynamic of multi-robot systems, multi-robot interaction and attack strategy, problem statement and event-triggered data transferring mechanism. In Section III, we design a SDECL for multi-robot systems in the presence of cyber attack. In Section IV, we analyze stochastic boundedness of the estimation error in mean square for the SDECL algorithm under cyber attacks. In Section V we present the case study including the simulation and experimental results. Finally, Section VI contains some conclusions of the results.

### II. PROBLEM STATEMENT AND PRELIMINARIES

#### A. DYNAMIC OF MULTI-ROBOT SYSTEMS

We consider a team of \( N \) mobile robots moving in the two-dimensional space. The general nonlinear motion of each
robot, \( i \in \mathbb{D} = \{1, 2, \ldots, N\} \), is described as follows ([5]):

\[
x^i(k) = f^i(x^i(k-1), u^i_m(k-1)),
\]

where the state vector \( x^i(k) = [x^i(k), y^i(k), \theta^i(k)]^T \) contains the position and orientation of each robot with respect to global map and \( u^i_m \) is the control input. Each robot interacts with inertial sensors to measure its linear velocity \( u^i_m = \dot{u}^i + \eta^i \), where \( \dot{u} \) represents the actual velocity and \( \eta^i \) is corresponding white-Gaussian noise. Each robot detect uniquely the other robots in the team using exteroceptive sensors and take relative measurements with respect to them, including range or bearing or a combination of these measurements. The relative measurement taken by robot \( i \) from robot \( j \) at a time \( k \) is described by ([5]):

\[
z_{ij}(k) = h_{ij}(x^i(k), x^j(k)) + \nu_{ij}(k),
\]

where \( h_{ij}(x^i, x^j) \) is the measurement model and \( \nu_{ij} \) is measurement noise. The noises \( \eta^i \) and \( \nu_j \) are independent white-Gaussian processes with known positive definite variances \( Q_i(k) = \mathbb{E}[\eta^i(k)\eta^i(k)^T] \) and \( R_j(k) = \mathbb{E}[\nu^j(k)\nu^j(k)^T] \). All noises are assumed to be mutually uncorrelated.

### TABLE 1. Notation.

| Notation | Description |
|----------|-------------|
| \( E \{ \} \) or \( \mathbb{E} \{ \} \) | expectation of the random variable |
| \( Tr(\cdot) \) | trace of the matrix |
| \( \text{diag}(\cdot) \) | block diagonal matrix |
| \( \| \cdot \| \) | Euclidean norm of the vector |
| \( \text{Prob}(\cdot) \) | occurrence probability of event \( \cdot \) |
| \( X^T \) | transpose of matrix \( X \) |
| \( X^{-1} \) | inverse of matrix \( X \) |
| \( \mathbb{R}^n \) | set of \( n \)-dimensional real vectors |
| \( 
\mathbb{S}^n \) | set of \( n \times n \) real matrices |
| \( I \) | identity matrix of appropriate dimensions |
| \( i \) | index of robot \( i \) and robot \( j \) |
| \( x^i(k) \) | state vector of the robot \( i \) (position and orientation) |
| \( u^i_m(k) \) | control input of robot \( i \) |
| \( \eta^i(k) \) | process noise from control input of robot \( i \) |
| \( \nu^i(k) \) | measurement noise from exteroceptive sensors for pair \((i, j)\) |
| \( \alpha_{ij}(k) \) | indicator of interaction between robots |
| \( \lambda_{ij} \) | set of neighbors of robot \( i \) within certain range |
| \( z^r_{ij}(k) \) | relative measurement taken by robot \( i \) from robot \( j \) |
| \( Q_i(k) \) | covariance of \( \eta^i(k) \) |
| \( R_j(k) \) | covariance of \( \nu^j(k) \) |
| \( A_i(k), G_i(k) \) | system matrix of robot \( i \) |
| \( H_i(k) \) | sensor measurement matrix of robot \( i \) |
| \( H^T_i(k) \) | sensor measurement matrix of robot \( i \) |
| \( l \) | \( l \) number of attacks launched to the communication links |
| \( \alpha^l_{ij}(k), \beta^l_{ij}(k) \) | random variables are employed for (sensor measurement) to determine whether the \((i, j)\)th communication channel (sensor-filter) is attacked by DoS and FDI at time \( k \) |
| \( \zeta^l_{ij}(k), \lambda^l_{ij} \) | random variables are employed (for propagated state) to determine whether the \((i, j)\)th communication channel (filter-filter) is attacked by DoS and FDI at time \( k \) |
| \( z^v_{ij}(k), \tilde{z}^v_{ij}(k) \) | random variables are employed (for event trigger) to determine whether the \((i, j)\)th communication channel (filter-filter) is attacked by DoS and FDI at time \( k \) |
| \( \tilde{P}^v_{ij}(k) \) | estimated state error covariance of robot \( i \) |
| \( \tilde{P}^{v}_{ij}(k) \) | estimated state error covariance of robot \( i \) |
| \( P^{v}_{ij}(k) \) | estimated state error covariance between robots \( i \) and \( j \) |
| \( K_i(k) \) | Kalman gain |
| \( \hat{\theta}^i(k), \hat{\theta}^j(k) \) | event-triggered parameters for pair \((i, j)\) |
| \( \gamma_{ij}(k) \) | decision variable (event-detector) used to decide whether or not the current relative measurement transmission occurs |
| \( \psi_{ij}(k) \) | attack detector parameter for pair \((i, j)\) |
| \( d_{ij}(k) \) | decision variable (attack detector) is used to decide whether or not the packets transmitted to the neighbors |
| \( \xi_{ij}^l(k) \) | attacker signal for \((i, j)\)th communication channel (sensor-filter) |
| \( \phi_{ij}^l(k) \) | attacker signal for \((i, j)\)th communication channel (filter-filter) |

### B. MULTI-ROBOT INTERACTION AND ATTACK STRATEGY

The interaction topology of robots is shown in Fig. 2. We assume that each robot can sense the other robots in the team and take relative measurements \( z_{ij}(k) \) and exchange information packets (propagated state and error covariance) with its neighboring robots residing within communication range. Since we have a set of \( N \) robots, we consider the interaction topology \( G = (V, E, L) \), where \( V = \{1, \ldots, N\} \) is the set of nodes in the graph. For each node \( v_i \), the index \( i \in \{1, 2, \ldots, N\} \) is the unique identifier of the agent \( i \). \( E \) represents the set of information links of the propagated estimates (state and error covariance) exchange between robots. \( L \subseteq \{a_{ij} \in \mathbb{R}^N \times N \} \) is the adjacency matrix of the propagated estimates (state and error covariance) interaction topology.

When \( a_{ij} \neq 0 \), robot \( i \) is able to receive information packets (propagated state and error covariance) from robot \( j \), while \( a_{ij} \neq 0 \) indicates that there is no information flow from the robot \( j \) to robot \( i \). Notice that the resulting network topology is time-varying and reflects the practical scenario in a multirobot system where robots can randomly sense the other robots in the team only within the reach of the exteroceptive sensors. Notice also that in this setup, measurement and communication links are identical. A robot \( j \) can exchange information packets with a neighbour robot \( i \), only within certain communication range with the robot \( i \) belongs to set \( N \subseteq \{ v \in V : (i, j) \in E \} \).

We consider that both DoS and FDI attacks can be randomly launched into the communication network and can arbitrarily block or manipulate sensor measurements and information exchange between robots. We assume that the number of attacks affecting the network is limited, in order to reflect the real-world adversaries. As Fig. 2 shows the attacker launch randomly \( l \in \Gamma = \{1, 2, \ldots M\} \) number of attacks at each time to the communication links (sensor measurements and estimates), where \( M \) is the maximum number of attacked links.

### C. PROBLEM STATEMENT

Fig. 1 shows the block diagram of the proposed SDECL algorithm. This scheme is based on our previous work [34], but has been modified to include cyber attacks. Here, each robot detects the other robots in the team using the exteroceptive sensors. The relative measurement \( z_{ij}(k) \) taken by each robot \( i \) is sent to the event detector which determines whether or not current sensor measurement is to be transmitted to the filter over the unreliable communication network, based on a triggering rule. The relative measurement transmitted by the event-detector to the corresponding filter may be tampered by malicious attackers. Both DoS and FDI attacks can block and contaminate the sensor measurements through wireless network which is described by [38]:

\[
\tilde{z}_{ij}^l(k) = \alpha_{ij}^l(k) \tilde{z}_{ij}(k) + (1 - \alpha_{ij}^l(k)) \beta_{ij}^l(k) \xi_{ij}^l(k),
\]

where the random variables \( \alpha_{ij}^l(k) \) and \( \beta_{ij}^l(k) \) are mutual independent Bernoulli distributed white sequences taking values
be applied to equations (4) and (5). Note that the adversaries
the unprotected communication channel. The exchanged
\( \alpha \) when
\( E \)
\( \theta \)
\( \psi \)
\( \nu \)
\( \chi \)
\( d \)
\( \gamma \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
\( \lambda \)
\( \sigma \)
\( \tau \)
\( \mu \)
\( \kappa \)
\( \zeta \)
\( \xi \)
\( \omega \)
\( \rho \)
\( \gamma \)
\( \tau \)
\( \alpha \)
\( \delta \)
\( \theta \)
\( \phi \)
\( \epsilon \)
\( \beta \)
where $\psi_{ij}$ is the preset threshold. It can be seen in Fig. 1 that the detector decide whether to trigger the alarm for the robot $i$ or not. The threshold $\psi_{ij}$ should be appropriately chosen to balance the false alarm rate and the detection accuracy [37]. In order to minimize the false alarm rate caused by the relative measurement noise, we set the detector threshold $\psi_{ij}$ to $3\sigma_{ij}$, where $\sigma_{ij}$ is the covariance of the relative measurement noise. As a result, by setting the detector threshold to $3\sigma_{ij}$, the probability of false alarm rate due to relative measurement noise can be reduced to 1%, the same value as in [36].

Remark 1: Multi-Robot System (MRS) refers to a team of robots that work cooperatively. By contrast, Multi-Agent System (MAS) refers to a more general system in which an agent is a general object which could be a robot, a drone, but may also be a cyber component, such as a software construct.

Remark 2: In a centralized event-triggered mechanism, it is assumed that there exists a global microprocessor, i.e., the host computer, that collects information (relative measurements) about the whole system and triggers feedback events for each robot. In the decentralized event-triggered mechanism, each robot is equipped with its own embedded microprocessor (micro-controller) that can take relative measurements only from neighboring robots within certain sensing range and trigger events based on received relative measurements. In the distributed event-triggered mechanism, the robots need to trigger the event immediately based on received relative measurements from all neighboring robots. In this work, we consider a decentralized event-triggered mechanism where each robot equipped with its own embedded microprocessor, take relative measurements from neighboring robots and independently trigger events according to the received measurements. Note that whether a system is centralized or decentralized is independent of whether this system is distributed or non-distributed. The main advantage of using a decentralized mechanism over centralized mechanism is that in the case of robot failure, all other robots can proceed unaffected. Also, the advantage of using non-distributed mechanism to distributed mechanism is that the event-triggered mechanism does not wait to receive relative measurements from all neighboring robots and can trigger based on the corresponding relative measurements received. This feature can improve filtering accuracy.

Remark 3: Notice that, in practice, attacks can occur randomly. To protect the system against attacks, the defender can estimate the probability and intensity of the attack signal using statistical tests by monitoring the attacker behaviour online for a period of time. It is therefore reasonable to assume that the probability and the bound of the attack signal are statistically known to the defender. Similar assumptions can be found in references [39], [40], [41].

Remark 4: We assume that all stochastic variables regarding the communication channel between exteroceptive sensors and robot’s filter ($\alpha_{ij}(k)$, $\beta_{ij}(k)$) are independent with the communication channel between two filters ($\xi_{ij}(k)$, $\lambda_{ij}(k)$, $\sigma_{ij}(k)$, $\tau_{ij}(k)$) in $i$, $j$ and $k$.

Remark 5: In reality, an attacker can typically only launch a limited number of attacks to the communication links among agents due to limited energy resources. Denoting $\Xi_{ij} \subseteq \mathbb{N}$ the set containing the measurement or communication links affected by attacks, then for $l$ number of attacked measurement links ($\alpha_{ij}(k) = 0 \forall (i,j) \in \Xi_{ij}$) and attacked communication links ($\xi_{ij}(k) = 0$ or $\sigma_{ij}(k) = 0 \forall (i,j) \in \Xi_{ij}$). In the FDI attack, it is assumed that the attacker knows the system model and employs a bounded signal to implement the attack. Notice that a bounded signal is preferred by the attacker due to the resource constraints. Moreover, if the attack signal has a large amplitude then it can be easily detected by the detector. Thus, a sophisticated attacker prefers to transmit a bounded false signal to degrade localization performance. It is therefore reasonable to assume that the false signals transmitted by attacker are bounded. Similar assumptions can be found in [31], [37], and [38].

Remark 7: There are other forms of stating the boundedness condition such the use of $L_1$, or $L_2$ norm used for systems with a bounded noise signal. In this work, however, we model noise as a Gaussian distribution. The fundamental problem here is that all the signals are stochastic with unbounded support (due to the Gaussianity assumption). Therefore, we may not simply assume that signals are bounded with probability 1 while simultaneously assuming that (related) the signals are Gaussian random variables. This is precisely the reason that we may not write (for example) that $\mathbf{E}_{ij}^l(k) = \mathbf{E}_{ij}^l(k)^T$ is bounded. Note also that, in the proofs, we do not need the signals themselves to be bounded. We only need their expectations/moments to be bounded. Therefore, it is better (and technically correct) to assume that $\mathbb{E}\left\{\mathbf{E}_{ij}^l(k) \mathbf{E}_{ij}^l(k)^T\right\}$ is bounded rather than imposing a deterministic bound on $\mathbf{E}_{ij}^l(k) \mathbf{E}_{ij}^l(k)^T$ itself.

D. EVENT-TRIGGERED DATA TRANSFERRING MECHANISM

In order to reduce the communication rate of sensors and therefore extending the battery life of mobile robots, the exteroceptive sensors is equipped with an event-triggered scheduler that decides when relative measurement transmission should occur. The event detector mechanism (7) is based on mixed triggered mechanism [31] which works as follows. Define now the binary decision variable $\gamma_{ij}(k)$:

$$
\gamma_{ij}(k) = \begin{cases} 
1, & \text{if } \left\|e_{ij}(k)\right\| \geq \Theta_{ij} \left\|z_{ij}(k)\right\| + \Lambda_{ij} \\
0, & \text{otherwise.}
\end{cases}
$$

(7)

where $z_{ij}(k)$ denotes the current sensor measurement, $\bar{z}_{ij}(k)$ represents the last measurement transmitted through the channel and $e_{ij}(k) = z_{ij}(k) - \bar{z}_{ij}(k)$ is the error between transmitted measurement (when triggered) and the current measurement at time $k$. $\Theta_{ij}, \Lambda_{ij} > 0$ are design parameters in the event-triggered mechanism. The smaller the value of $\Theta_{ij}, \Lambda_{ij}$, the more events are triggered, which results in higher demands on communication resources and higher
energy consumed by each robot. When the parameters $\Theta_{ij}$, $\Delta_{ij} > 0$ are sufficiently small, the event-triggered mechanism perform as a time-triggered system. From Eq. (7), we see that, the measurement $z_{ij}(k)$ will be sent to the estimator through unreliable communication channel if and only if $y_{ij}(k) = 1$.

### III. DESIGN OF A SDECL UNDER CYBER ATTACK

In this section, we design a SDECL algorithm via extended Kalman filter (EKF) with event-triggered mechanism (7) and considering cyber attacks (3)-(5). Firstly, we derive the prediction error and estimation error covariances. Then, we obtain the upper bound of the estimation error covariance by employing a stochastic analysis. Finally, we derive the Kalman gain for the proposed filter by minimizing the estimation error covariance. Before we proceed further, we introduce the following Lemma which will be used to obtain our results:

**Lemma 1:** For any two vectors $x, y \in \mathbb{R}^n$, there exists a scalar $\epsilon \in \mathbb{R}$ such that the following inequality holds [39]:

$$xy^T + xy^T \leq \epsilon xx^T + e^{-1}yy^T. \tag{8}$$

**Theorem 1:** Consider the nonlinear discrete-time system (1) and (2) with the event-triggered communication strategy (7). Assume that the relative measurement $(\hat{z}_{ij}(k), \tilde{z}_{ij}(k))$ and the predicted belief $\text{bel}^{-}(k) = (\hat{x}^{-}, \hat{P}^{-})$, $\text{bel}^{+}(k) = (\hat{x}^{+}, \hat{P}^{+})$ are affected by DoS and FDI attacks (3)-(5) in the unreliable communication channels. For the secure CL via the EKF, the upper bound of estimation error covariance can be obtained as follows:

$$P^{ij}(k) = C_1 \Phi_{ij}(k) P^{ij-}(k) \Phi_{ij}^T(k) + C_2 \Phi_{ij}^T(k) \Phi_{ij-}(k) P^{ij-}(k) \Phi_{ij}^T(k)$$

Finally, we derive the Kalman filter (EKF) with event-triggered mechanism (7)

$$\Phi_{ij}^-(k) = A_i(k-1) \Phi_{ij}^+(k-1) A_i(k-1)^T + G_i(k-1) Q_i(k-1) G_i(k-1)^T$$

**Proof:** The proof is given in the Appendix A. \(\square\)

**Remark 8:** It is important to notice that it is impossible to compute the actual value of the estimation error covariance due to some terms $E\left\{ \sum_{j \in \mathcal{N}_i} \Phi_{ij}^T(k) \Phi_{ij}(k) [\hat{x}^+(k)^T \Phi_{ij}^+ T(k)] \right\}$.
and also
\[ F_{ij}(k) = \sum_{j \in \mathcal{N}_i} a_{ij}(k) \mathbb{E} \left[ \tilde{w}_{ij}(k)^T \right] \Delta_{ij}(k) X_i(k)^T \]

Remark 9: In Corollary 1, we obtain the optimal Kalman filter gain for the proposed filter by minimizing the trace of the upper bound of the estimation error covariance. Considering the structure of the optimal Kalman gain in (10)-(12), the event-triggered mechanism and cyber-attacks introduce additional parameters affecting the upper and lower bounds of the estimation error and the estimation error covariance. Moreover, in the absence of the attack, the optimal gain in (10)-(12) is the same as the one in [34]. Also, note that the proposed filter is suboptimal due to parameters of the cyber attacks, the event-triggered mechanism, and the topology of the interaction between robots. In order to improve the filter’s performance, the parameters \( \epsilon_1, \epsilon_2, \ldots \) can be tuned in a way that the upper bound of estimation error covariance is minimized further. Specifically, the parameters \( \epsilon_1, \epsilon_2, \ldots \) can be obtained by an optimization algorithm (genetic algorithm) in the MATLAB code “[x, f, min] = ga(f(x), n, v, …)”, where \( f(x) \) is the objective function (upper bound of error covariance) to be optimized and \( n \) is the dimension of \( f(x) \). Note that similar approach can be found in [24].

IV. BOUNDEDNESS OF ESTIMATION ERROR FOR THE PROPOSED SDECL

In this section, we analyze the resilience of the proposed filter under cyber attacks. We derive sufficient conditions that ensure convergence and stochastic stability of the proposed filter.

Lemma 2: ([32]) Assume there is a stochastic process \( V_k(\pi_k) \) as well as real numbers \( \kappa, \bar{\kappa}, \mu > 0 \) and \( 0 < \phi \leq 1 \) such that
\[ \kappa \|\pi_k\|^2 \leq V_k(\pi_k) \leq \bar{\kappa} \|\pi_k\|^2 \]
and
\[ \mathbb{E}[V_k(\pi_{k-1})] - V_{k-1}(\pi_{k-1}) \leq \mu - \phi V_{k-1}(\pi_{k-1}) \]
are satisfied. Then the stochastic process is exponentially bounded in mean square sense, i.e.,
\[ \mathbb{E}\left[\|\pi_k\|^2\right] \leq \frac{\kappa}{\mu} \mathbb{E}\left[\|\pi_0\|^2\right] (1 - \phi)^k + \frac{\mu}{\kappa} \sum_{n=1}^{k-1} (1 - \phi)^n \]
and the stochastic process is bounded with probability one.

Assumption 1: There exist real constants \( a_i, \bar{a}_i, \bar{h}_i, \bar{h}_i, \bar{h}_{ij}, \bar{a}_{ij}, \bar{q}_{ij}, \bar{R}_{ij}, \bar{g}_{ij}, \bar{g}_i > 0 \) such that the following bounds on various matrices are satisfied for every \( k \geq 0 \):
\[ a_i \leq \|A_k(k)\| \leq \bar{a}_i, \quad h_i \leq \|H_i(k)\| \leq \bar{h}_i, \]
\[ h_{ij} \leq \|H_{ij}(k)\| \leq \bar{h}_{ij}, \quad q_{ij} \leq \|Q_{ij}(k)\| \leq \bar{q}_{ij}, \]
\[ R_{ij} \leq \|R_{ij}(k)\| \leq \bar{R}_{ij}, \quad g_{ij} \leq \|G_{ij}(k)\| \leq \bar{g}_{ij}. \]

Theorem 2: Assume that the nonlinear discrete-time system (1) and (2) with the event-triggered communication strategy (7) and random cyber attacks (3-5) satisfies Assumption 1. Given \( \bar{p}_i \leq P^{ij}(0) \leq \bar{p}_i \) and \( \bar{p}_{ij} \leq P_{ij}(0) \leq \bar{p}_{ij} \) where \( \bar{p}_i, \bar{p}_j, \bar{p}_{ij} \) are known positive values. If the following inequality is satisfied,
\[ \sigma_1 + 2\sigma_2^2 \left( C_1 \bar{p}_i \tilde{F}_{ij, \max} \right) \left( r_{ij, \min}^{-1} - r_{ij, \min}^{-1} C_1 \tilde{F}_{ij, \min} \bar{F}_{ij, \max} \right) \left( \sum_{j \in \mathcal{N}_i} \tilde{p}_j \phi_{ij, \max} \right) T \]
\[ + \sigma_3^2 \left( C_1 \bar{p}_i \tilde{F}_{ij, \max} \right) \left( r_{ij, \min}^{-1} C_1 \tilde{F}_{ij, \min} \bar{F}_{ij, \max} \right) T \]
\[ - r_{ij, \max}^{-1} C_1 \tilde{F}_{ij, \min} \bar{F}_{ij, \max} \left( \sum_{j \in \mathcal{N}_i} \tilde{p}_j \phi_{ij, \max} \right) T \leq \bar{p}_i \]
then the filtering error covariance is exponentially bounded in mean square sense.
\[
\tilde{d}_{ij} = \begin{cases} 
\{d_{ij}\}_{j \in N_i} & \text{max}(\psi_{ij}), \\
\{d_{ij}\}_{j \in N_i} & \text{min}(\psi_{ij})
\end{cases}
\]

\[
\bar{\mathbf{y}}_i \leq E\left[\mathbf{y}_i\right] \leq \tilde{\mathbf{y}}_i
\]

\[
\tilde{F}_{ij,\text{max}} = \sum_{j \in N_i} \tilde{d}_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{max}} \tilde{h}_{ij}, \quad \tilde{F}_{ij,\text{min}} = \sum_{j \in N_i} d_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{min}} h_{ij}
\]

\[
\tilde{\Phi}_{ij,\text{max}} = \tilde{d}_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{max}} \tilde{h}_{ij}, \quad \tilde{\Phi}_{ij,\text{min}} = d_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{min}} h_{ij}
\]

\[
F_{ij} = \frac{\tilde{d}_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{max}} \tilde{h}_{ij}}{\tilde{\Phi}_{ij,\text{max}}}, \quad \tilde{\Phi}_{ij,\text{min}} = \frac{d_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{min}} h_{ij}}{\tilde{\Phi}_{ij,\text{min}}}
\]

\[
\phi_{ij}^k = \frac{\tilde{d}_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{max}} \tilde{h}_{ij}}{\tilde{\Phi}_{ij,\text{max}}}, \quad \phi_{ij}^k = \frac{d_{ij} \tilde{a}_{ij} \tilde{\phi}_{ij,\text{min}} h_{ij}}{\tilde{\Phi}_{ij,\text{min}}}
\]

\[
r_{ij,\text{max}} = \sum_{j \in N_i} \tilde{F}_{ij,\text{max}} \tilde{p}_{ij,\text{max}} \tilde{F}_{ij,\text{max}}^T + \sum_{j \in N_i} \tilde{\Phi}_{ij,\text{max}} \tilde{p}_{ij,\text{min}} \tilde{F}_{ij,\text{min}}^T + C_2 \sum_{j \in N_i} \tilde{\Phi}_{ij,\text{max}} \tilde{p}_{ij,\text{min}} \tilde{p}_{ij,\text{min}}^T
\]

then, the inequality \( \mathbf{p}_i \leq \mathbf{P}^{i+}(k) \leq \mathbf{P}^{i-}(k) \leq \tilde{\mathbf{p}}_i \) holds for any \( k \geq 1 \).

**Proof**: The proof is given in the Appendix B. \( \square \)

Remark 10: In Theorem 2, we provide a sufficient condition for the convergence and resilience of the proposed filter using mathematical induction and matrix analysis. It is important to notice that condition (16) includes all terms involving the dynamics of multi-robot system (MRS), event-triggered mechanism, cyber attacks, communication topology as well as attack detector. In practice, the boundary of MRS in Assumption 1, the bound of the attacker signal and its probability, and the interaction of robots can be estimated by the defender using parameter identification. Note that if the bound of attack signals \( (\xi_{ij}, \tilde{d}_{ij}, \text{etc}) \) are large, the estimation error covariance increases according to condition (16), then \( r_{ij,\text{max}} \) will increase, resulting in an increase of the upper bound of estimation error covariance. Also, the parameters \( \Theta_{ij}, \Lambda_{ij} > 0 \) of the event-triggering mechanism in Eq. (7) affect the upper bound of the estimation error covariance. From (7), we can see that the average communication rate \( \mathbf{v}_{ij} \) decreases as the value of \( \Theta_{ij}, \Lambda_{ij} \) increase. Moreover, based on (16), we can see that \( r_{ij,\text{max}} \) will increase as the value of \( \Theta_{ij}, \Lambda_{ij} \) increase. Therefore, we conclude that the upper bound of error covariance increases with the value of \( \Theta_{ij}, \Lambda_{ij} \). Conversely, smaller the values of \( \Theta_{ij}, \Lambda_{ij} \) result in more data transmission. It follows from (16) that the upper bound of the error covariance would be decreased and better estimation performance would be expected at the cost of imposing heavy burden on the communication channels. These two scenarios lead to a tradeoff in the value of \( \Theta_{ij}, \Lambda_{ij} \) to balance between the estimation performance and reduced network transmission. When, both parameters of the event triggered mechanism \( \Theta_{ij}, \Lambda_{ij} \) and those of the adversary signal \( (\xi_{ij}, \tilde{d}_{ij}, \text{etc}) \) are large, the estimation error covariance might diverge. Convergence and resilience of the proposed filter is guaranteed provided that the attack signals, event-triggered parameters, etc., satisfy inequality (16). If upper bound of the estimation error covariance converges asymptotically with \( k \), then the error covariance must converge as well.

Remark 11: The parameter \( \psi_{ij} \) of the detection mechanism in Eq. (6) affects the performance of the proposed filter.
TABLE 2. Value and description of the parameters in simulation.

| Parameters | Description | Value |
|------------|-------------|-------|
| b          | Distance between wheels | 0.5   |
| N          | Number of robots         | 4     |
| Q₁         | Standard deviation of control input | (0.05)^2 diag((ΔL₁)^2, (ΔP₁)^2) |
| R_ij       | Standard deviation of relative measurements | diag([0.1m^2, 0.1rad^2]) |
| P₀⁺(0), P⁺(0) | Initial covariance matrix | diag([0.15^2, 0.15^2]) |

When the sensor measurements of robot j are under malicious attack, the data received from robot j, namely, propagated state and error covariance, is suspicious and then the detector may trigger the alarm by setting d_{ij}(k) ≠ 0 (representing a presence of attack) to avoid the transmission of the packets to other robots. As a result the detection mechanism reduces the impact of malicious attack and improves the performance of the filter. Note that the defender may design the detector threshold (ψ_{ij}) in order to minimize the missing attack report rate, assuming knowledge of the boundary of the MRS in Assumption 1, the bound of attacker signals and its probability, the interaction of robots, event-triggered parameters. Note that the estimation error covariance in the SDECL algorithm does not represent the actual estimation error exactly. Therefore, the result of Theorem 2 can be employed to analyze the performance of the estimation error. This is done in our next Theorem.

Theorem 3: Consider the nonlinear discrete-time system (1) and (2) with the event-triggered communication strategy (7) and random cyber attacks (3-5). If

\[ \hat{P}⁺(k) ≤ P⁻(k) ≤ \hat{P}_i \]

and for some εi > 0, \( E \left\{ ||\hat{x}⁺(0)||^2 \right\} \leq ε_i \), then the estimation error \( \hat{x}⁺(k) = x⁺(k) - \hat{x}⁺(k) \) is exponentially bounded in mean square for any i ∈ Ø.

Proof: The proof is given in the Appendix C. □

Remark 12: According to Theorem 3, the upper bound of \( \hat{P}_{ij}(k) \) in (50) depends on the event-triggered threshold, parameters of cyber attack (sensor-filter and filter-filter communication channels) which affects on the upper bound of \( E \left\{ ||\hat{x}⁺(k)||^2 \right\} \). Thus, by assuming bounded attacker signal (DoS and FDI) and choosing a proper event triggered condition, one can limit the upper bound of filtering error.

V. CASE STUDY
A. SIMULATION RESULTS
In this subsection the performance of the proposed SDECL algorithm (1) under cyber attacks is verified by simulation results. The motion equations of the i-th robot is described by:

\[
\begin{align*}
  x^i(t + 1) &= x^i(t) + Δn^i(t) \cos(θ^i(t)) + Δθ^i(t) \\
  y^i(t + 1) &= y^i(t) + Δv^i(t) \sin(θ^i(t)) + Δθ^i(t) \\
  θ^i(t + 1) &= θ^i(t) + Δω^i(t)
\end{align*}
\]

Algorithm 1 A Secure Decentralized Cooperative Localization Algorithm Under Cyber Attack

1: Initialize state estimation and error covariance matrix as:

\[
\begin{align*}
  \hat{x}⁺(0) ∈ ℜ^d, \quad P⁺(0) ∈ ℜ^{d×d}, \quad P⁺(0) = 0_{d×d}
\end{align*}
\]

2: repeat

3: Propagation: Compute the predicted state and error covariance for each robot:

\[
\begin{align*}
  \hat{x}⁻(k) &= f(\hat{x}⁺(k) - 1), \quad u_{i,m}(k - 1) \\
  P⁻(k) &= A_i(k - 1)P⁺(k - 1)A_i(k - 1)^T + G_i(k - 1)Q_i(k - 1)G_i(k - 1)^T
\end{align*}
\]

4: Update:

5: if robot i ∈ Ø detect the other robot in the team, the relative measurement \( z_{ij}(k) \) taken by each robot will sent to event-detector to judge whether to transmit the current measurement or not through unprotected communication network. Then, each robot exchange propagated state and error covariance with the other robot through unreliable communication network. The arriving innovation and its covariance considering cyber attacks are as follows:

\[
\begin{align*}
  Y_j(k) &= a_j(k)z_j(k) + (1 - a_j(k))b_j(k)ξ_j(k) \\
  S_j(k) &= C_jF_j(k)P⁻(k)F_j(k)^T + \sum_{i∈N_j} C_iF_i(k)P⁻(k)F_j(k)^T + \sum_{i∈N_j} C_iF_i(k)P⁻(k)F_j(k)^T + C_jR_j(k)Φ_j(k)\hat{Φ}_j(k)^T + \sum_{i∈N_j} C_iR_i(k)Φ_j(k)\hat{Φ}_j(k)^T + \sum_{i∈N_j} C_iR_i(k)Φ_j(k)\hat{Φ}_j(k)^T + C_jR_j(k)Φ_j(k)\hat{Φ}_j(k)^T + \sum_{i∈N_j} C_iR_i(k)Φ_j(k)\hat{Φ}_j(k)^T
\end{align*}
\]

- If arriving innovation is greater than the threshold, i.e., \( \|Y_j(k)\| ≥ Ψ \) → attack detected → trigger the alarm
- If arriving innovation is less than the threshold, i.e., \( \|Y_j(k)\| < Ψ \) → proposed filter is resilient against cyber attacks → follow steps 6-9

6: Compute optimal Kalman gain under cyber attacks:

\[
K_j(k) = \left[ C_jP⁻(k)F_j(k) + \sum_{i∈N_j} F_i(k)\hat{Φ}_j(k)\hat{Φ}_j(k)^T \right]^{-1}S_j(k)
\]

7: Update state estimation with the current measurement:

\[
\hat{x}_j(k) = \hat{x}⁺(k) + K_j(k)\sum_{i∈N_j} Y_j(i)
\]

8: Update the error covariance:

\[
\begin{align*}
  P⁺(k) &= P⁻(k) - K_j(k)S_j(k)K_j(k)^T \\
  P⁻(k) &= P⁻(k) - K_j(k)S_j(k)K_j(k)^T
\end{align*}
\]

9: \( k ← k + 1 \)

where \( x^i(t) ∈ ℜ^d \) and \( y^i(t) ∈ ℜ^d \) are the Cartesian coordinates of robot i, \( θ^i(t) ∈ ℜ^d \) is the orientation, \( v^i(t) \) and \( ω^i(t) \) are the linear velocity and angular velocity, respectively. Denote \( u^i(t) = [ΔL_i, ΔR_i]^T \), where \( ΔL_i \) and
T. Kargar Tasooji, H. J. Marquez: SDECL in Multi-Robot Systems Under Cyber Attack

FIGURE 3. (a) Localization of 4 robots by SDECL algorithm under event-triggered mechanism without cyber attack; (b)-(d) Localization of 4 robots by SDECL algorithm under different triggering conditions and with cyber attack; (e)-(j) the triggering instances for the range and bearing of the four robots; solid-o shows the ground truths, broken-dot shows the dead-reckoning and broken-x shows the EKF estimates of 4 robots.

FIGURE 4. 1) Position estimation error of each robot using SDECL algorithm for different scenarios; the brown curve shows under event-triggered mechanism and without cyber attacks, the red, blue and green curves show under different triggering conditions and with cyber attacks; 2) The pink color shows the position estimation error of each robot using classical CL algorithm under event-triggered mechanism and with cyber attacks.

\[ \Delta R_i \text{ are distance moved by wheels. Note that, the control input of each robot } i \text{ is measured by odometry and inertial sensors. Also, the relative measurements taken by robot } i \in \{1, 2, 3, 4\} \text{ from robot } j \in \{1, 2, 3, 4\} \setminus \{i\} \text{ is described by:} \]

\[ z_{ij}(t) = \begin{bmatrix} \rho_{ij}(t) \\ \theta_{ij}(t) \end{bmatrix} = \begin{bmatrix} \sqrt{(x^i(t) - x^j(t))^2 + (y^i(t) - y^j(t))^2} \\ \arctan\left(\frac{y^i(t) - y^j(t)}{x^i(t) - x^j(t)}\right) \end{bmatrix} \tag{19} \]

where:

- \( \rho_{ij}(t) \) is the range of robot \( i \) relative to the robot \( j \).
- \( \theta_{ij}(t) \) is the bearing of the robot \( i \) relative to the robot \( j \).

We assume that additive white-Gaussian noise affects both the control input \( u^i(t) \) and the relative measurements \( z_{ij}(t) \). In a practical application, this noises may account for the effect of model uncertainties associated with the wheel encoders and overhead camera. In our simulations, we compare the following: 1) Ground truth of each robot; 2) Localization of robots using filter propagation; 3) Localization of robots using the SDECL algorithm 1 with/without cyber attacks.

In our simulations we assume that the mobile robots move in a random trajectory and at least one of them perform as a stationary robot. Robots then employs their exteroceptive sensors to observe the stationary robot and take relative measurements. We consider a scenario in which the filter corresponding to each robot receives information through an unreliable communication network. The moving robots then receive the predicted position and associated error covariance of each observed stationary robot over the unreliable
communication network. An adversary can attempt to attack the communication between the sensor and filter of each robot and between two filters and degrade the localization quality. Fig. 3, Fig. 4, Fig. 5 and Fig. 6 show the outcome of our simulation results. We first evaluate the performance of dead-reckoning method where each robot employs only the wheel-encoders to estimate the pose (position and orientation) independently with no exchange of information (estimated states and error covariance) with other robots. As seen in Fig. 3 that pose estimation error using dead-reckoning method grow continuously for each robot, showing that using only local information (i.e. using only wheel-encoder information) is ineffective to determine the location of each robot in the team. Next we consider the scenario in which each robot receives continuous (i.e. time-triggered) relative measurements through a reliable communication network, without cyber attacks, and correct its pose estimation. As seen in Fig. 3(a), the pose estimation from SDECL algorithm closely tracks the reference trajectory (ground truths). Fig. 3(e) and Fig. 3(f) indicate the triggering instances with respect to time for the range and bearing of each robot. Note that the absence of triggering times in the case of time-triggered mechanism means that the robot i performs as a stationary robot for the rest of robots.

Then, we simulate a scenario that includes mixed DoS and FDI attacks with probability of 0.2 and 0.2 (both of attacks) applied to the communication channel between the exteroceptive sensors and corresponding estimator. In other words, we consider the case in which each robot receives relative measurement intermittently (with event-triggered mechanism) in an unreliable communication network (with mixed DoS and FDI attacks) and correct its pose estimation using
FIGURE 8. Localization of 4 robots by SDECL algorithm (a) under event-triggered mechanism without cyber attack; (b) with event-triggered mechanism and in the presence of DoS attacks; (c) with event-triggered mechanism and in the presence of FDI attacks.

FIGURE 9. Position estimation error of each robot using SDECL algorithm for different scenarios.

the proposed algorithm (1). Fig. 3(b), Fig. 3(c) and Fig. 3(d) show that when the event-triggering parameters increases for the same rate of DoS and FDI attacks, the quality of the tracking deteriorates slightly, however the tracking error remains bounded. Fig. 3(g) and Fig. 3(h) display the triggering times corresponding to event-triggering condition used in Fig. 3(c) and also Fig. 3(i) and Fig. 3(j) indicate the triggering instances corresponding to event-triggering condition used in Fig. 3(d). To compare the filter performance under different triggering conditions we use position error for each robot. According to Fig. 4, we conclude that our proposed algorithm (1) outperforms the classical CL under cyber attacks. Also, by properly tuning the triggering condition for the given attack rate, we can achieve good estimation while reducing the communication rate. Then we consider the filter’s performance under the following assumptions: (i) no attacks; when there is an attacks affecting one of the following: (ii) communication between the sensor measurements and the robot’s filter, (iii) communication between filters; (iv) communication between the sensor measurements and the robot’s filter and between the filters. The results are shown in Fig. 5(a), Fig. 5(b), Fig. 5(c) and Fig. 5(d). We consider mixed DoS and FDI attacks with the probability of 0.1 and 0.1 applied in cases (ii), (iii) and (v). Also, the parameters of the event-triggering conditions are the same in all cases. Fig. 5(e) and Fig. 5(f) shows the triggering times corresponding to the event-triggering condition used in Fig. 5(a), Fig. 5(b), Fig. 5(c) and Fig. 5(d). Finally we evaluate the performance of the filter by comparing the position error for all cases. We conclude that although the position error slightly increases in case (v) with respect to case (ii) and case (iii), the proposed filter still remains resilient against simultaneous attacks and considering reduced amount of range-bearing measurements. We also illustrate the performance of proposed SDECL algorithm (i) without cyber-attacks, (ii) under DoS attacks, (iii) under FDI attacks. It can be seen from Fig. 8 and Fig. 9 that our algorithm is efficient in each of these scenarios. Then we simulate the false alarm rate and missing report rate with different detector parameters. Fig. 7 shows the relationship between the false alarm rate and the missing report rate versus detector parameter. It can be seen that false alarm rate decreases when the detector threshold is increased, while the missing report rate increases when the detector threshold is increased. In other words, a small false alarm rate can be interpreted as the detector judging that normal relative measurements are untrustworthy, whereas a higher rate of missing report can be interpreted that the detector judging that falsified relative measurements are credible.

B. EXPERIMENTAL VALIDATION

In this subsection we validate the performance of the SDECL algorithm by performing experiments on our robotic system. Our setup (see Fig. 10) consists of a Linux-based host computer equipped with Nvidia GPU, four e-puck2 mobile robots, an overhead ZED stereo camera and the workspace of robots. The system is equipped with Robot Operating System.
TABLE 3. Value and description of the parameters in experiment.

| Parameters | Description | Value |
|------------|-------------|-------|
| $d$        | Distance between wheels | 0.053m |
| $N$        | Number of robots | 4 |
| $Q_i$      | Standard deviation of control input | $(0.05)^2 \text{diag}([\Delta L_i^2], (\Delta R_i^2)]$ |
| $R_i$      | Standard deviation of relative measurements | $\text{diag}([0.03, 5^\circ])]$ |

($\text{ROS}$) where each robot and the overhead camera correspond to a ROS node. Our computer vision system [33] tracks the pose of each robot with respect to the reference trajectory and also provides relative measurements. The accuracy of the computer vision-based positioning algorithm is $0.03m$ for range and $5$ degree for bearing. E-puck2 robots move along circular trajectory simultaneously with a radius of $0.13$ m (see Fig. 12). Each e-puck2 is equipped with odometry sensor to propagate the filter. The host computer uses the ZED camera to collect data from the four e-puck2 robots and produce relative measurements (range and bearing) using computer vision software. The event detector uses the corresponding relative measurements to decide whether or not new information is to be transmitted to the robots. When a pair of robots receives new relative measurements, they exchange information (propagated state and error covariance) with each other to update the localization. The communication between e-puck2 robots and the host computer is conducted through Bluetooth. There is inherent time delays in communication between two robots, the camera latency and image processing and the event-detector. Also, the ROS package message_filter [42] is used to synchronize the time stamp of the odometry data and relative measurements. We perform two experiments as following:

1) LOCALIZATION OF ROBOTS UNDER CYBER ATTACKS

In this experiment, we compare the following: 1) A ground truth of each robot provided by the overhead ZED camera; 2) Localization of robots by odometry sensor; 3) Localization of robots using the SDECL algorithm 1 considering cyber attacks. Fig. 11 shows the results of our experiments. In our experiments, the trajectory generated by the overhead camera is employed as our reference trajectory. Note that the odometry sensor provides the pose estimates for the filter propagation. Each robot uses range-bearing measurements to improve the localization accuracy. Fig. 11(a) and Fig. 11(b) shows the performance of SDECL algorithm under time-triggered and event-triggered mechanisms where packets transmitted in a reliable communication network. It can be seen that

FIGURE 11. Trajectories of the e-puck2 robots under an experimental test generated by four simultaneously running ROS packages, one for the camera location tracking (the green curve), one for the odometry estimate (the red curve), and the other one (the blue curve) to obtain location estimates by SDECL Algorithm (a) under time-triggered mechanism and without cyber attacks; (b) under event-triggered mechanism and without cyber attacks; (c) under event-triggered mechanism and bounded cyber attacks.
the event-triggered mechanism achieves a trade-off between localization accuracy and number of transmitted packets. Fig. 11(c) shows the resiliency of proposed SDECL algorithm in the presence of bounded attack. We assume mixed DoS and FDI attacks with probabilities of 0.1 and 0.1 corrupting the sensor measurements in the sensor-filter communication channel. In this case, we assume that the attacker blocks and manipulates the relative measurement obtained from the camera in the communication channel between the exteroceptive sensors and the filter. It can be seen that the cyber attack deteriorates the localization accuracy slightly but still the proposed algorithm is resilient against bounded attacks. We also provide the position error of the four e-puck2 robots (see Fig. 11) by comparing (i) time-triggered mechanism without cyber attacks; (ii) event-triggered mechanism without cyber attacks; (iii) event-triggered mechanism with cyber attacks. We conclude that the our algorithm provides satisfactory localization performance against cyber attacks while reducing the amount of transmitted range-bearing measurements.

2) CYBER ATTACK DETECTION

In this experiment, we apply mixed DoS and FDI attacks to corrupt the transmitted relative measurement of e-puck0 under unbounded attack signal. Since, the attack detector monitors the filter by checking the arriving innovation, an alarm is triggered if the arriving innovation is greater than the threshold. Note that the LEDs of the e-pucks turn on when the alarm triggers, indicating the presence of a possible attack. Fig. 14(a)-(d) shows the status of e-pucks at \( t = 0, 7, 13, 20 \) s. According to the SDECL algorithm, all robots communicate with each other, in order to perform localization. When one of the robots receives corrupted sensor measurements, the corrupted packets (propagated state and error covariance) are transmitted to the other robots, thus increasing the norm of the arriving innovation and eventually triggering an alarm. It can be seen from Fig. 14(a)-(d) that the LEDs of all robots turn on as alarm since the corrupted packets (propagated state and error covariance) received from e-puck0 increase the arriving innovation of other robots and trigger the alarm indicating a possible attack. In Fig. 14(e)-(h) we consider the proposed attack detection mechanism. Here the alarm of e-puck0 is triggered indicating an attack, thus, the robot does not transmit the corrupted packets to the other robots. Therefore, we can see that the arriving innovation in the other robots is less than the threshold resulting in an improvement in the localization performance.
VI. CONCLUSION
In this article, we study the problem of event-triggered cooperative localization with the specific objective of cyber attacks. For the attacks with limited resources, we design the optimal Kalman filter under both DoS and FDI attacks, and provided a sufficient condition to guarantee the convergence and resilience of the proposed filter. Moreover, we also propose an attack detection mechanism for the proposed algorithm when the attack signal are unbounded. Simulation and experimental results show the efficiency of the proposed algorithm. As mentioned earlier, in cooperative localization exteroceptive and proprioceptive sensors need to be fused to correct the navigation states. More specifically, laser, camera and IMU sensors usually run at different sampling rates, leading to sensor data streams being multi-rate. To tackle this case, multi-rate EKF should be use to estimate the position of robots. Further research will include the extension of our results to the multi-rate EKF-based localization algorithm for multi-robot systems subject to network-induced phenomena (e.g. asynchronous communication, DoS attacks [19], deception attacks [16], [17], etc) and unknown measurement sensitivity [20].

APPENDIX A
PROOF OF THEOREM 1
Proof: The predicted state error of robot $i$ for MRS (1) at time instant $k + 1$ can be described by:
$$\tilde{x}^i(k + 1) = x^i(k + 1) - \hat{x}^i(k + 1)$$  (20)
where the predicted state of each robot $\hat{x}^i(k + 1)$ is defined by:
$$\hat{x}^i(k + 1) = f^i(\hat{x}^i(k), u^i_m(k))$$  (21)
Expanding $f^i(\hat{x}^i(k), u^i_m(k))$ using Taylor series around $\hat{x}^i(k)$, we have:
$$f^i(\hat{x}^i(k), u^i_m(k)) \approx f^i(\hat{x}^i(k), u^i_m(k)) + A_i(k)(\hat{x}^i(k) - \hat{x}^i(k)) + o(\hat{x}^i(k))$$  (22)
where $A_i = \frac{\partial f^i(\hat{x}^i, u^i_m)}{\partial x^i}$ and $o(\hat{x}^i(k))$ denote the high-order terms of the Taylor series expansion. Following [31], [39], we introduce the unknown time-varying matrix $F_j(k)$, and known scaling matrix $B_j(k)$ to account for the linearization error. We can write:
$$o(\hat{x}^i(k)) = B_i(k)F_i(k)E_i(k)\hat{x}^i(k)$$  (23)
where $E_i(k)$ is a known tuning matrix and assume that $F_i(k)$ satisfies:
$$F_i(k)F_i(k)^T \leq I$$  (24)
Defining $A_i(k) = A_i(k) + B_i(k)F_i(k)E_i(k)$ and using (20)-(23), the predicted state error for robots $i$ and $j$ can be computed as follows:
$$\tilde{x}^i(k + 1) = A_i(k)\tilde{x}^i(k) + G_i(k)\eta_i(k)$$  (25)
where $G_i = \frac{\partial f^i(\hat{x}^i, u^i_m)}{\partial x^i}$, $G_j = \frac{\partial f^j(\hat{x}^j, u^j_m)}{\partial x^j}$, and $A_i = \frac{\partial f^i(\hat{x}^i, u^i_m)}{\partial x^i}$. Using Eqs. (25)-(26), the predicted state error covariance for robot $i$ and cross covariance between two robots ($i$ and $j$) are represented by:
$$P^i(k + 1) = \mathbb{E}[(\tilde{x}^i(k + 1))(\tilde{x}^i(k + 1))^T] = A_i(k)P^i(k)A_i(k)^T + G_i(k)Q_i(k)G_i(k)^T$$  (27)
$$P^ij(k + 1) = \mathbb{E}[(\tilde{x}^i(k + 1))(\tilde{x}^j(k + 1))^T] = A_i(k)P^ij(k)A_j(k)^T$$  (28)
Considering the event-triggered mechanism (7) and random cyber attack (3), the current transmitted measurement is as follows (for simplicity of the notation we use time instant $k$ instead of time instant $k + 1$):
$$\tilde{y}_0^i(k) = \alpha^i_0(k)\left(z_0^i(k) - (1 - \gamma_0^i(k))e_0^i(k)\right) + (1 - \alpha^i_0(k))\beta^i_0(k)\xi_0^i(k)$$  (29)
The arriving innovation can be computed as follows:
$$\gamma_0^i(k) = \alpha^i_0(k)\left(z_0^i(k) - (1 - \gamma_0^i(k))e_0^i(k)\right) + (1 - \alpha^i_0(k))\beta^i_0(k)\xi_0^i(k) - h_0^i(\tilde{x}^i(k), \tilde{u}^i(k))$$  (30)
The state estimates of each robot are corrected according to:
$$\hat{x}^i(k) = \tilde{x}^i(k) + K_i(k)\left[\sum_{j \in N_i} d_{ij}(k)a_{ij}(k)(\tilde{z}_0^j(k) - h_j(\tilde{x}^j(k), \tilde{u}^j(k)))\right]$$  (31)
where $h_j(\tilde{x}^j, \tilde{u}^j)$ is the predicted measurement. Let the first-order expansion of $h_j(\tilde{x}^j, \tilde{u}^j)$ around $(\tilde{x}^j, \tilde{u}^j)$ be
$$h_j(\tilde{x}^j, \tilde{u}^j) \approx h_j(\hat{x}^j, \hat{u}^j) + H_j(\tilde{x}^j - \hat{x}^j) + H'_j(\tilde{u}^j - \hat{u}^j) + o(\tilde{x}^j(k), \tilde{u}^j(k))$$  (32)
where $H_j = \frac{\partial h_j(\tilde{x}^j, \tilde{u}^j)}{\partial x^j}$, $H'_j = \frac{\partial h_j(\tilde{x}^j, \tilde{u}^j)}{\partial u^j}$ and $o(\tilde{x}^j(k), \tilde{u}^j(k))$ represent the high-order terms of the Taylor series expansion. We now introduce unknown time-varying matrices $C_j(k)$ and $C'_j(k)$, and known scaling matrices $D_j(k)$ and $D'_j(k)$ accounting for the linearization errors of the measurement model:
$$o(\tilde{x}^j(k), \tilde{u}^j(k)) = D_j(k)C_j(k)E_j(k)\tilde{x}^j(k)$$  (31)
where $E_i^j(k)$ and $E_j^i(k)$ are known tuning matrices and assume that $C_i^j(k)$ and $C_j^i(k)$ satisfy:

$$C_i^j(k)C_i^j(k)^T \preceq I \quad \text{(34)}$$
$$C_j^i(k)C_j^i(k)^T \preceq I \quad \text{(35)}$$

Note that the matrices $D_i^j(k)$, $D_j^i(k)$, $E_i^j(k)$, $E_j^i(k)$, $B_i(k)$ and $E_j(k)$ should be designed appropriately. Substituting (29) into (31), we have:

$$\dot{x}^i(k) = \dot{x}^i(k) + K_i(k)\left[\sum_{j \in N_{i_{ij}}} d_{ij}(k) a_{ij}(k) \left(\alpha_{ij}(k) \left(\tilde{z}_0(k) \right) + (1 - \gamma_{ij}(k))e_{ij}(k) + (1 - \alpha_{ij}(k))\beta_{ij}(k)\tilde{e}_{ij}(k) \right) - h_{ij}(k) \left(\dot{x}^i(k), \dot{x}^i(k)\right)\right]$$

Using (32)-(36) and introducing $H_i^j(k) = H_i^j(k) + D_i^j(k)C_i^j(k)E_i^j(k)$, $H_j^i(k) = H_j^i(k) + D_j^i(k)C_j^i(k)E_j^i(k)$ the estimation error can be computed as follows:

$$\dot{\tilde{x}}^i(k) = x^i(k) - \dot{\tilde{x}}^i(k) = \Phi_{ij}^0(k)\tilde{x}^-i(k)$$

where

$$\Phi_{ij}^0(k) = \left(I - K_i(k)\sum_{j \in N_{i_{ij}}} d_{ij}(k) a_{ij}(k) \alpha_{ij}(k)H_i^j(k) \right)$$

Using (37), the estimation error covariance matrix can be computed as follows:

$$P_i^k(k) = \mathbb{E}\left\{\dot{\tilde{x}}^i(k)\dot{\tilde{x}}^i(k)^T\right\}$$

$$= \mathbb{E}\left\{\Phi_{ij}^0(k)\tilde{x}^-i(k)\dot{\tilde{x}}^-i(k)^T\right\}$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{x}^-i(k)\right]$$

$$\times \left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{x}^-i(k)^T\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)w_{ij}(k)^T\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)h_{ij}(\cdot)^T\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{e}_{ij}(k)^T\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{e}_{ij}(k)\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{e}_{ij}(k)^T\right] K_i(k)^T$$

$$+ K_i(k)\mathbb{E}\left[\sum_{j \in N_{i_{ij}}} \Phi_{ij}^0(k)\tilde{e}_{ij}(k)\right] K_i(k)^T$$
where covariance matrix in (27) and substituting $\mathbf{K}_i(k)$ in (10)-(12) we write:

$$
P^{i-}(k + 1) = \mathcal{A}_i(k) \left[ \mathbf{P}^{i-}(k) - \left( C_i \mathbf{P}^{i-}(k) \bar{F}_j(k) \right) \right]
+ \sum_{j \in N_i} \mathbf{P}^{ij-}(k) \bar{F}_j(k) \right) \mathbf{K}_i(k)^T \right] \mathcal{A}_i(k)^T
+ \mathcal{G}_i(k) \mathbf{Q}_j(k) \mathbf{G}_j(k)^T
= \mathcal{A}_i(k) \left[ \mathbf{P}^{i-}(k) - \left( C_i \mathbf{P}^{i-}(k) \bar{F}_j(k) \right) \right]
+ \sum_{j \in N_i} \mathbf{P}^{ij-}(k) \bar{F}_j(k) \right) \mathbf{K}_i(k)^T \right] \mathcal{A}_i(k)^T
+ \mathcal{G}_i(k) \mathbf{Q}_j(k) \mathbf{G}_j(k)^T
(41)
$$

where

$$
r_j(k) = \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_2 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_3 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_4 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_5 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_6 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ C_7 \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
+ \sum_{j \in N_i} \bar{F}_j(k) \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T
(42)
$$

Using the inequality $(A + B)^{-1} > A^{-1} - A^{-1}BA^{-1}$ we write:

$$
P^{i-}(k + 1) \leq \mathcal{A}_i(k) \left[ \mathbf{P}^{i-}(k) \mathcal{A}_i(k)^T + \mathcal{A}_i(k) \left( C_i \mathbf{P}^{i-}(k) \bar{F}_j(k) \right) \right]
\times \left[ r_j(k)^T - r_j(k) \mathcal{A}^{-1}_i \bar{F}_j(k) \mathbf{P}^{i-}(k) \right]
\times \left( C_i \mathbf{P}^{i-}(k) \bar{F}_j(k) \right)^T \mathcal{A}_i(k)^T
+ \mathcal{A}_i(k)
\times \left( \sum_{j \in N_i} \mathbf{P}^{ij-}(k) \bar{F}_j(k)^T \right)^T
$$

Defining constants $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6, \epsilon_7, \epsilon_8, \epsilon_9 > 0$ and applying Lemma 1 we obtain an upper bound of the error covariance matrix (9), which completes the proof. □

**VII. PROOF OF THEOREM 2**

Proof: It is obvious that the state estimation error and the error covariance matrix are updated with new relative measurement. The updated error covariance can be computed as follows:

$$
P^{i+}(k) = \mathbf{P}^{i-}(k) - \mathbf{K}_i(k) \mathbf{S}_{i,a}(k) \mathbf{K}_i(a)^T
(39)
$$

$$
P^{ij+}(k) = \mathbf{P}^{ij-}(k) - \mathbf{K}_i(k) \mathbf{S}_{i,a}(k) \mathbf{K}_i(a)^T
(40)
$$

where $\mathbf{S}_{i,a}(k)$ is covariance of arriving innovation which can be obtained from Eq. (12). So, we can show that $\mathbf{P}^{i+}(k + 1) \leq \mathbf{P}^{i-}(k + 1)$. Considering the prediction error covariance matrix in (27) and substituting $\mathbf{K}_i(k)$ in (10)-(12) we write:
\[
\begin{align*}
&\times [r_{ij}^{-1}(k) - r_{ij}^{-1}(k)C_1\tilde{F}_{ij}(k)P^{ij}(k)] \\
&\times \left( C_1P^{ij}(k)\tilde{F}_{ij}(k) \right)^T A_i^T(k) + A_i(k) \\
&\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right) \\
&\times \left( r_{ij}^{-1}(k) - r_{ij}^{-1}(k)C_1\tilde{F}_{ij}(k)P^{ij}(k) \right) \\
&\times \left[ C_1P^{ij}(k)\tilde{F}_{ij}(k) \right]^T A_i^T(k) + A_i(k) \\
&\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right)^T A_i^T(k) + A_i(k) \\
&\times \left( C_1P^{ij}(k)\tilde{F}_{ij}(k) \right)^T A_i^T(k) + 2A_i(k) \\
&\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right) \\
&\times \left( r_{ij}^{-1}(k) - r_{ij}^{-1}(k)C_1\tilde{F}_{ij}(k)P^{ij}(k) \right) \\
&\times \left[ C_1P^{ij}(k)\tilde{F}_{ij}(k) \right]^T A_i^T(k) + A_i(k) \\
&\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right) \\
&\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right)^T A_i^T(k) + A_i(k) \\
&+ A_i(k)P^{ij}(k)A_i^T(k)
\end{align*}
\]
}

Therefore, we show that the error covariance matrix is bounded for \( k \geq 1 \) by mathematical induction, which completes the proof.

**APPENDIX C**

**PROOF OF THEOREM 3**

Proof: First, we choose the Lyapunov function as follows:

\[
V_k(\hat{x}^{i+(k)}) = \hat{x}^{i+(k)}^T \left( P^{i+(k)} \right)^{-1} \hat{x}^{i+(k)}
\]

Using Theorem 2 it is obtained that \( pI \preceq P^{i+(k)} \preceq \hat{p}I \). According to the condition in (16), the Lyapunov function Eq. (45) is bounded according to the following inequality:

\[
\frac{1}{\hat{p}} \| \hat{x}^{i+(k)} \|^2 \leq V_k(\hat{x}^{i+(k)}) \leq \frac{1}{p} \| \hat{x}^{i+(k)} \|^2
\]

Next, we have to ensure the boundary of \( \mathbb{E}\left[ V_k(\hat{x}^{i+(k)}) \right] \) \( \hat{x}^{i+(k)}(k-1) - V_{k-1}(\hat{x}^{i+(k)}(k-1)) \). On the basis of Eq. (45), the conditional expectation \( \mathbb{E}\left[ V_k(\hat{x}^{i+(k)}) \right] \) \( \hat{x}^{i+(k)}(k-1) \) is derived:

\[
\begin{align*}
\mathbb{E}\left[ V_k(\hat{x}^{i+(k)}) \right] & = \mathbb{E}\left[ \hat{x}^{i+(k)}(k-1)^T A_i(k-1) \tilde{F}_{ij}(k)^T \right. \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T P^{i+(k)} \left. \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k)
\end{align*}
\]

Considering the property of conditional expectation that \( \mathbb{E}\left[ \hat{x}^{i+(k)}(k) \right] = \hat{x}^{i+(k)}(k) \), the following equation is obtained by subtracting \( V_{k-1}(\hat{x}^{i+(k)}(k-1)) \) from Eq. (47):

\[
\begin{align*}
\mathbb{E}\left[ V_k(\hat{x}^{i+(k)}) \right] & = \mathbb{E}\left[ \hat{x}^{i+(k)}(k-1) \right] \\
& - V_{k-1}(\hat{x}^{i+(k)}(k-1)) \\
& \times \left[ A_i(k-1) \tilde{F}_{ij}(k)^T \right. \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T P^{i+(k)} \left. \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
& \times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k)
\end{align*}
\]

Now, in order to prove the boundedness of error covariance \( P^{i+(k)}(k+1) \), we assume that \( \tilde{p}I \preceq P^{i+(k)}(k) \preceq \hat{p}I \) and \( pI \preceq P^{ij}(k) \preceq \tilde{p}I \) holds at \( k \), then we will show that it is true in \( k+1 \).

\[
P^{i+(k)}(k+1) \leq \tilde{a_i}^2 \tilde{p}_i + 2\tilde{a_i}^2 \left( C_1\tilde{p}_i\tilde{F}_{ij}(k)_{\text{max}} \right) \\
\times \left[ r_{ij}^{-1}(k) - r_{ij}^{-1}(k)C_1\tilde{F}_{ij}(k)P^{ij}(k) \right] \\
\times \left( \sum_{j \in N_i} P^{ij}(k)\Phi_{ij}(k)^T \right) \\
\times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
\times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k) \\
\times \left( \tilde{F}_{ij}(k)^T \right)^T A_i(k)
\]

(44)
According to Eqs. (10)-(12), the following inequality for Kalman gain is given as:

\[
\|K_i(k)\| \leq \left( C_1 \tilde{p}_{ij,\text{max}} + \sum_{j \in N_i} \tilde{p}_{ij} \tilde{\Phi}_{ij,\text{max}}^2 \right) \times \left( C_1 \tilde{\xi}_{ij,\text{min}} P_{ij,\text{min}}^{-1} r_{ij,\text{min}} \right) = \tilde{K}_i
\]

Both sides of \( \mu_{ij}(k) \) are scalars. Using Lemma 1 and computing the trace of \( \mu_{ij}(k) \), we have:

\[
\tilde{\mu}_{ij}(k) \leq \text{Tr} \left\{ \sum_{j \in N_i} \left[ A_j(k - 1)^T \tilde{\Phi}_{ij,\text{max}}^2 K_i(k)^T \right] \right\} + \text{Tr} \left\{ \sum_{j \in N_i} \left[ \tilde{\Phi}_{ij,\text{max}}^2 K_i(k) \right] \right\}
\]

According to Lemma 2, there is

\[
\tilde{K}_i \leq \frac{1}{\kappa} \frac{A}{\kappa} \left( \sum_{j=1}^{k-1} \tilde{\mu}_{ij} \right)^2
\]

This completes the proof. 

REFERENCES

[1] J. A. Fax and R. M. Murray, “Information flow and cooperative control of vehicle formations,” IEEE Trans. Autom. Control, vol. 49, no. 9, pp. 1465–1476, Sep. 2004.

[2] S. I. Roumeliotis and G. A. Bekey, “Distributed multilot localization,” IEEE Trans. Robot. Autom., vol. 18, no. 5, pp. 781–795, Oct. 2002.

[3] K. B. Purvis, K. J. Astrom, and M. Khanshah, “Estimation and optimal configurations for localization using cooperative UAVs,” IEEE Control Syst. Technol., vol. 16, no. 5, pp. 947–958, Sep. 2008.

[4] F. Morbidi and G. L. Mariottini, “Active target tracking and cooperative localization for teams of aerial vehicles,” IEEE Trans. Control Syst. Technol., vol. 21, no. 5, pp. 1694–1707, Sep. 2013.

[5] J. Zhu and S. S. Xia, “Cooperative localization under limited connectivity,” IEEE Trans. Robot., vol. 35, no. 6, pp. 1523–1530, Dec. 2019.

[6] A. I. Mourikis and S. I. Roumeliotis, “Performance analysis of multirobot cooperative localization,” IEEE Trans. Robot., vol. 22, no. 4, pp. 666–681, Aug. 2006.

[7] L. Zhou and P. Tokere, “Active target tracking with self-triggered communications in multi-robot teams,” IEEE Trans. Autom. Sci. Eng., vol. 16, no. 3, pp. 1085–1096, Jul. 2019.

[8] X.-G. Guo, D.-Y. Zhang, J.-L. Wang, J. H. Park, and L. Guo, “Observer-based event-triggered composite anti-disturbance control for multi-agent systems under multiple disturbances and stochastic FDIAs,” IEEE Trans. Autom. Sci. Eng., early access, Mar. 31, 2022, doi: 10.1109/TASE.2022.3162651.

[9] G. Bianchin, Y.-C. Liu, and F. Pasqualetti, “Secure navigation of robots in adversarial environments,” IEEE Control Syst. Lett., vol. 4, no. 1, pp. 1–6, Jan. 2020.

[10] Y. Mo and B. Sinopoli, “Secure estimation in the presence of integrity attacks,” IEEE Trans. Autom. Control, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Trans. Autom. Control, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[12] Y. Shoukry and P. Tabuada, “Event-triggered state observers for sparse sensor noise/attacks,” IEEE Trans. Autom. Control, vol. 61, no. 8, pp. 2079–2091, Aug. 2016.
H. Lin, J. Lam, and Z. Wang, “Secure state estimation for cyber-physical systems: A game-theoretic approach,” IEEE Trans. Autom. Control, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

F. Q. E. Tian, and X. Zhao, “Chance-constrained $H_{\infty}$ state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case,” IEEE Trans. Neural Netw. Learn. Syst., early access, Jan. 7, 2022, doi: 10.1109/TNNLS.2021.313742.

S. Zhu, E. Tian, D. Xu, and J. Liu, “An adaptive torus-event-based $H_{\infty}$ controller design for networked T-S fuzzy systems under deception attacks,” Int. J. Robust Nonlinear Control, vol. 32, no. 6, pp. 3425–3441, 2022, doi: 10.1002/rnc.5957.

Y. Pan, Q. Li, H. Liang, and H.-K. Lam, “A novel mixed control approach for fuzzy systems via membership functions online learning policy,” IEEE Trans. Fuzzy Syst., vol. 30, no. 9, pp. 3812–3822, Sep. 2022, doi: 10.1109/TFUZZ.2021.3130201.

Y. Pan, Y. Wu, and H.-K. Lam, “Security-based fuzzy control for nonlinear networked control systems with DoS attacks via a resilient event-triggered scheme,” IEEE Trans. Fuzzy Syst., vol. 30, no. 10, pp. 4359–4368, Oct. 2022, doi: 10.1109/TFUZZ.2022.3148875.

H. Liang, Z. Du, T. Huang, and Y. Pan, “Neuroadaptive performance guaranteed control for multiagent systems with power integrators and unknown measurement sensitivity,” IEEE Trans. Autom. Control, vol. 67, no. 6, pp. 2843–2856, Jun. 2022, doi: 10.1109/TAC.2021.3092603.

Y. Chen, S. Kar, and J. M. F. Moura, “Resilient distributed estimation: Sensor attacks,” IEEE Trans. Autom. Control, vol. 64, no. 9, pp. 3772–3779, Sep. 2019.

L. An and G.-H. Yang, “Distributed secure state estimation for cyber-physical systems under sensor attacks,” Automatica, vol. 107, pp. 526–538, Sep. 2019.

A.-Y. Lu and G.-H. Yang, “Secure state estimation for multiagent systems with faulty and malicious agents,” IEEE Trans. Autom. Control, vol. 65, no. 8, pp. 3471–3485, Aug. 2020.

L. Su and S. Shahamzour, “Finite-time guarantees for Byzantine-resilient distributed state estimation with noisy measurements,” IEEE Trans. Autom. Control, vol. 65, no. 9, pp. 3758–3771, Sep. 2020.

A.-Y. Lu and G.-H. Yang, “Distributed secure state estimation in the presence of malicious agents,” IEEE Trans. Autom. Control, vol. 66, no. 6, pp. 2875–2882, Jun. 2021.

M. Quinet, D. Iglesias, N. Ahmed, and S. Martínez, “Cooperative robot localization using event-triggered estimation,” J. Aerosp. Inf. Syst., vol. 15, no. 7, pp. 427–449, Jul. 2018.

D. P. Borgers and W. P. M. H. Heemels, “Event-separation properties of event-triggered control systems,” IEEE Trans. Autom. Control, vol. 59, no. 10, pp. 2644–2656, Oct. 2014.

K. Reif, S. Günther, E. Y. Zay, and R. Unbehauen, “Stochastic stability of the discrete-time extended Kalman filter,” IEEE Trans. Autom. Control, vol. 44, no. 4, pp. 714–728, Apr. 1999.

R. M. Salinas and B. Magyar. (2015). ArUco ROS Library. [Online]. Available: http://wiki.ros.org/aruco

T. K. Tasojo and H. J. Marquez, “Cooperative localization in mobile robots using event-triggered mechanism: Theory and experiments,” IEEE Trans. Autom. Sci. Eng., vol. 19, no. 4, pp. 3246–3258, Oct. 2022, doi: 10.1109/TASE.2021.3115770.

T. K. Tasojo and H. J. Marquez, “Decentralized event-triggered cooperative localization in multirobot systems under random delays: With/without timestamps mechanism,” IEEE/ASME Trans. Mechatronics, early access, Sep. 13, 2022, doi: 10.1109/TMECH.2022.3203439.

K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” IEEE Trans. Control Netw. Syst., vol. 1, no. 4, pp. 370–379, Dec. 2014.

J. Huang, Y. Tang, W. Yang, and F. Li, “Resilient consensus-based distributed filtering: Convergence analysis under stealthy attacks,” IEEE Trans. Ind. Informat., vol. 16, no. 7, pp. 4878–4888, Jul. 2020.

S. Liu, G. Wei, Y. Song, and Y. Liu, “Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks,” Neurocomputing, vol. 207, pp. 708–716, Sep. 2016.

L. Li, H. Yang, Y. Xia, and H. Yang, “Event-based distributed state estimation for linear systems under unknown input and false data injection attack,” Signal Process., vol. 170, May 2020, Art. no. 107423.

H. Gao, H. Dong, Z. Wang, and F. Han, “Recursive minimum-variance filter design for state-saturated complex networks with uncertain coupling strengths subject to deception attacks,” IEEE Trans. Cybern., vol. 52, no. 10, pp. 11121–11132, Oct. 2022, doi: 10.1109/TCYB.2021.3067822.

D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” IEEE Trans. Ind. Informat., vol. 15, no. 5, pp. 2483–2499, May 2019.

S. Liu, G. Wei, Y. Song, and Y. Liu, “Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks,” Neurocomputing, vol. 207, pp. 708–716, Sep. 2016.

L. Li, H. Yang, Y. Xia, and H. Yang, “Event-based distributed state estimation for linear systems under unknown input and false data injection attack,” Signal Process., vol. 170, May 2020, Art. no. 107423.

H. Gao, H. Dong, Z. Wang, and F. Han, “Recursive minimum-variance filter design for state-saturated complex networks with uncertain coupling strengths subject to deception attacks,” IEEE Trans. Cybern., vol. 52, no. 10, pp. 11121–11132, Oct. 2022, doi: 10.1109/TCYB.2021.3067822.

D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” IEEE Trans. Ind. Informat., vol. 15, no. 5, pp. 2483–2499, May 2019.