Research Article

On the Security of Data Collection and Transmission from Wireless Sensor Networks in the Context of Internet of Things

Hong Yu, Jingsha He, Ruohong Liu, and Dajie Ji

1 College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
2 School of Software Engineering, Beijing University of Technology, Beijing 100124, China
3 General Administrative Department, Beijing Development Area Co., Ltd., Beijing 100176, China
4 Information and Technology Center, Hebei Normal University for Nationalities, Chengde, Hebei 067000, China

Correspondence should be addressed to Jingsha He; jhe@bjut.edu.cn

Received 5 February 2013; Revised 21 August 2013; Accepted 21 August 2013

Academic Editor: Muhammad Khurram Khan

Copyright © 2013 Hong Yu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the context of Internet of Things (IoT), multiple cooperative nodes in wireless sensor networks (WSNs) can be used to monitor an event, jointly generate a report and then send it to one or more Internet nodes for further processing. A primary security requirement in such applications is that every event data report be authenticated to intended Internet users and effectively filtered on its way to the Internet users to realize the security of data collection and transmission from the WSN. However, most present schemes developed for WSNs don’t consider the Internet scenario while traditional mechanisms developed for the Internet are not suitable due to the resource constraint of sensor nodes. In this paper, we propose a scheme, which we refer to as Data Authentication and En-route Filtering (DAEF), for WSNs in the context of IoT. In DAEF, signature shares are generated and distributed based on verifiable secret sharing cryptography and an efficient ID-based signature algorithm. Our security analysis shows that DAEF can defend against node compromise attacks as well as denial of service (DoS) attacks in the form of report disruption and selective forwarding. We also analyze energy consumption to show the advantages of DAEF over some comparable schemes.

1. Introduction

To become an indispensable part of the Internet of Things (IoT), wireless sensor networks (WSNs) need to adopt IP technologies to create a seamless, global network infrastructure together with the Internet. To achieve this goal, many standardization organizations have been actively pursuing standardization work for creating a global sensor network infrastructure [1, 2]. In the context of the IoT, any IP-enabled node in the Internet shall be able to communicate directly with any remote sensor node in a WSN that is used to monitor specific events. Data transmission from any WSN node to any Internet node can be event-driven, whose scenarios include events that may be sensed sporadically by multiple cooperative sensor nodes when something happens, for example, when detecting fire or door-opening, or can be scheduled at predefined intervals, for example, reporting temperature every two hours. To monitor specific events of interest, more than one sensor node can be used to collect data and transmit it via multihop wireless paths to one or more Internet nodes to improve robustness, especially in an environment in which security threats resulting from internal and external attacks due to node compromises is a serious concern. Under such circumstances, it is still required that data report be sent to one or more of the intended Internet users as accurately as possible.

Since sensor nodes in a WSN may be deployed in an unattended environment, as shown in Figure 1, attackers can relatively easily compromise one or more sensor nodes so that they can be used to inject false event data (e.g., compromised node A can report false data for the event) or disrupt the transmission of legitimate event data (e.g., compromised node B can temper or even discard true data for the event within the multi-hop forwarding process). If undetected, such attacks can cause not only the generation of false alarms but also the depletion of limited energy in the sensor nodes. Moreover, Internet users may not be notified
of a real event quickly and handle the event in time to avoid serious consequences. Therefore, it becomes imperative that security services such as data authenticity and availability be provided to resist such attacks.

In many critical applications, the data that are collected by sensor nodes can also be sensitive. Therefore, it is important to ensure data authenticity to detect the report of false or nonexisting events. If a report for an event can be collectively endorsed by multiple sensor nodes, data authenticity can be ensured in the sense that a certain number of compromised nodes cannot collectively forge a report. That is, to forge a valid report for an event, a larger number of nodes have to be compromised.

Moreover, since denial of service (DoS) attacks can occur as the result of corrupted partial endorsements or discarded true data for the event, authentication alone may not be sufficient. It thus requires that data availability measures be employed in addition to those for authenticity to make the security measures highly resilient to DoS attacks. End-route filtering of false data is vital in saving scarce network resources and in prolonging the life of the network.

Consequently, to achieve security objectives, it is evident that authentication and efficient en-route filtering of data from WSN nodes to one or more Internet users be developed to detect false data injection and to fight against DoS attacks.

Traditional detection mechanisms developed for the Internet usually rely on infrastructure equipment (e.g., firewalls) to filter out distributed denial of service (DDoS) packets, which is deemed to be not adequate for WSNs due to the resource-constrained characteristics of sensor nodes as well as the lack of a comparable infrastructure in WSNs. Meanwhile, current detection mechanisms developed for WSNs rely primarily on the use of predistributed keys shared between sensor nodes and the sink node, which cannot be directly applied to the IoT scenario since the data of the event sensed by cooperative sensor nodes is sent only to one local sink rather than to one or more Internet users who are usually situated in different locations, even in different networks, and who may not be able to establish shared keys with every sensor node to authenticate the event data from a sensor node.

In this paper, we propose a data authentication and en-route filtering (DAEF) scheme to ensure the security of data collection and transmission from WSNs in the context of IoT. In DAEF, we make use of verifiable secret sharing cryptography to distribute the shares based on the most efficient ID-based signature scheme to multiple cooperative sensor nodes. In the case of a node compromise, with the tolerance of an adversary’s compromising multiple neighboring nodes in the event area, the event report should be collectively generated, digitally signed, and forwarded to one or more of the intended Internet nodes through multipath routing. The main contributions of this paper are summarized as follows.

(1) After identifying the security requirements on data collection and transmission from WSNs in the context of IoT, we propose a secure and efficient solution to deal with the security problems which have not been sufficiently dealt with in existing solutions.

(2) We propose a data authentication and en-route filtering scheme, referred to as DAEF, without requiring the use of any preshared keys between the Internet users and the sensor nodes. Furthermore, not only can the scheme tolerate node compromise attacks, but it can also mitigate the impact of DoS attacks while minimizing energy consumption for the WSNs.

(3) We analyze some exiting data en-route filtering mechanisms proposed for WSNs with respect to their characteristics and limitations and compare them with DAEF.

(4) We illustrate how DAEF can be used as a secure and efficient mechanism to counter report disruption attacks to WSNs, a capability that we have not found so far in the literature.

(5) We conduct performance comparison between DAEF and some comparable schemes to demonstrate DAEF’s advantages over those schemes in terms of energy consumption, making DAEF suitable for WSNs.

The rest of this paper is organized as follows. In the next section, we review some related work on data authentication and en-route filtering. In Section 3, we present our proposed scheme, which includes assumptions, threat model and design goals, two preliminaries, and finally the procedure of the scheme. In Section 4, we analyze our proposed scheme in terms of security and performance and compare it to some comparable schemes. Finally, in Section 5, we conclude this paper in which we also discuss some future work.

2. Related Work

2.1. Authentication Frameworks for IoT. There are currently some authentication frameworks for data reports designed
specifically for WSNs in the IoT scenario. Oliveira et al. proposed the Secure-TWS scheme to authenticate the communication from a single node to multiple users by using certificate-based signature in which the certificate authority (CA) is part of the existing infrastructure in the Internet and, hence, is easy to provide since the Internet users only trust the CA and do not have to allow the CA to impersonate as themselves [3]. When the users receive a data report signed by a sensor node, they download the sensor node’s public key and the corresponding certificate from the CA to authenticate the report using signature verification. Yasmin et al. proposed a framework for authenticated broadcast/multicast by the sensor node using the identity-based online/offline signature (IBOOS) scheme [4]. The offline phase performs most of the signature computations to calculate the partial signature which is stored on sensor nodes. Whenever a sensor node reports an event, it performs minor computations to obtain the final signature based on the partial signature stored on it.

The above two schemes can enable all sensor nodes in the WSNs to send messages to report critical situations and allow every node on the path from the sender node to the receiver users to verify and filter out false data as early as possible without using any shared keys. The computation overhead of the first scheme is lower than that of the second, but it requires higher communication cost due to the transmission of certificates.

However, these two schemes do not take into consideration of the existence of compromised nodes that may inject false event data as well as can disrupt the transmission of legitimate event data. Firstly, an event may be reported by a single sensor node which may have been compromised but not yet detected, the false report can get propagated to the users who may then mistakenly take incorrect measures. Secondly, should there be a compromised node in the routes to the Internet users, the users might be misled or might even not be able to receive any messages. Therefore, it is necessary to use multiple surrounding sensor nodes to collectively generate a legitimate data report which should also be forwarded to the Internet users via multipath routing.

2.2. Authentication Based on Symmetric Cryptography in WSNs. In WSNs, the problem of authenticating an event report collected by multiple sensors to the local sink node has attracted a great deal of attention in recent years [5–20]. Most of the schemes achieve the goals through using message authentication codes (MAC) based on symmetric keys. The basic idea is to attach MACs to the event reports and to ensure that a legitimate report must have a certain number of valid MACs. When the event report is forwarded to the sink along a routing path, intermediate nodes can detect and drop a forge report if it does not carry enough number of valid MACs. SEF [5] and IHA [6] are two such schemes for filtering injected false data in WSNs. SEF allows both the sink node and the en-route nodes to authenticate a report that has \( T \) MACs generated by a cluster attached to it with a certain probability by using the keys from different partitions in a global key pool. IHA verifies a report that has \( T (T = t + 1) \) MACs and one compressed MAC attached that are computed by the cluster lead node in a deterministic and hop-by-hop fashion through using pairwise keys between two upper or lower associated nodes that are \( T \) hops away. All the following schemes are based on this \( T \)-authentication fashion, but on different technologies to be achieved. In DSF [7], dual key-sharing is used, that is, the random keys sharing and the associated keys sharing, to reduce the number of hops for the forwarded false data. In RAS [8], dynamic authentication tokens from one-way hash chain are used based on a predesigned partition-overlapping key pool scheme. In KAEF [9], a one-way key chain authentication method is used to generate and verify endorsements for transferred data. In STEF [10], the query response operation mode is adopted and the concept of ticket is proposed based on lightweight one-way functions so that messages are only forwarded if they contain a valid ticket that is originally issued by the base station. In PCREF [11], polynomials stored in each node are adopted, including an authentication polynomial and a check polynomial derived from the primitive polynomial, and used for endorsing and verifying the reports. In DEF5 [12], the so-called Hill Climbing approach is used to ensure that nodes close to a source cluster hold more keys for the source cluster than those that are further away to balance the network. In GPREF [13], a multiaxis division based approach for deriving location-aware keys is used. In DREF [14], an authentication scheme capable of filtering invalid messages, called CFA [21], and a novel idea of embedding proximity information into a Bloom filter prepared for the query purpose are employed. In EAB [15], an en-route authentication bitmap is developed by using the Bloom filter techniques to build an authentication manifest. In BECAN [16], a bandwidth-efficient cooperative authentication scheme is proposed based on random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique. Last, but not the least, in LBRS [17] and LEDS [18], location-based keys are utilized to authenticate a data report to prevent compromised nodes from breaking the entire WSN even though a certain area of the WSN may have been affected.

2.3. Authentication Based on Asymmetric Cryptography in WSNs. Some asymmetric cryptographic schemes, such as CCEF [19], PDF [20], and LTE [22], that rely on signature approaches can enable any report, not just the report that is sent to the sink node, to be authenticated and en-route filtered. Moreover, they do not require any preshared keys. CCEF employs a commutative cipher based on public key cryptography filtering mechanism in which cluster nodes can establish a secret association with the sink on a per-session basis, while the en-route nodes are equipped with a witness key to be used to verify the authenticity of reports without knowing the original session key. PDF leverages Shamir’s threshold cryptography and elliptic curve cryptography (ECC) to reject false data packets while LTE makes use of identity-based cryptography (IBC) based on bilinear pairing to bind the private key of each sensor node to both its identity and geographic location.

2.4. Critical Analysis and Comparison of Existing Schemes. Although the existing schemes can effectively perform the
functionality of authentication and false data report filtering, there are still some limitations in different aspects, such as key-sharing limitation, $T$-threshold limitation, node location limitation, static route limitation, lack of tolerance to report disruption attacks, lack of tolerance to selective forwarding attacks, to name a few. The notion of such limitations is discussed below.

(1) Key-sharing limitation refers to the requirement that every node that generates a report must share key material with the sink.

(2) $T$-threshold limitation refers to the situation in which the compromise of more than $T$-authentication partitions would put the whole WSN in danger. Such a limitation makes the network less resilient to the increase in the number of compromised nodes.

(3) Node location limitation refers to the requirement that each node be equipped with GPS capability to locate itself since only rough estimation on the location can be achieved for sensor nodes that are not equipped with GPS.

(4) Static route limitation refers to the reality in which reports get forwarded to a fixed sink along a preestablished path and each en-route node is associated with the source nodes in the event area.

(5) Lack of tolerance to report disruption attacks refers to the situation in which intentional submission of corrupted partial MACs or signatures by compromised sensor nodes would disrupt the process of data filtering by some sensor nodes on the forwarding route, also called packet pollution attacks or false-endorsement based DoS (FEDoS) attacks [23].

(6) Lack of tolerance to selective forwarding attacks refers to the situation in which one or more compromised forwarding sensor nodes can drop a legitimate report, also called path-based DoS (PDoS) attacks [24].

Table 1 provides an analysis on the limitations of some of the main existing schemes. We can see from the table that all symmetric key-based schemes exhibit the key-sharing limitation since it is practically infeasible for every remote user to establish a shared key with each and every one of the sensor nodes. Therefore, these symmetric keys based schemes are not suitable for WSNs in the context of IoT. A result, only PDF and LTE that are asymmetric cryptography-based signature schemes can be used for event data authentication and filtering in the IoT scenario. However, PDF suffers from the vulnerability of both report disruption attacks and selective forwarding attacks. Only DREF, LEDS, and LTE can resist report disruption attacks and selective forwarding attacks that result from node compromises in the event area and from the use of a single route from a sensor node to the sink node. The result of the analysis shows that only LTE is applicable to the IoT scenario and can provide some level of tolerance to both types of DoS attacks. Therefore, we will compare our proposed scheme in terms of performance only to LTE at the same security level.

2.5. Location-Based Threshold-Endorsement (LTE) Mechanism. Due to its functional capability as well as its applicability to the IoT scenario, we would like to elaborate a little more on the LTE scheme. In LTE, the sensor network is divided into $M \times N$ square cells of equal side length $r$. Each cell is labeled with a pair of integers $(m, n)$, where $1 \leq m \leq M$ and $1 \leq n \leq N$. $(X_0, Y_0)$ is the location of the sink. The cell key of cell $(m, n)$ is $K_{mn} = k(H(m \parallel n)$ where $k$ is the network master secret key. Let $ID^j_{mn}$ denote the $j$th node with location $l^j_{mn}$ in cell $(m, n)$. LTE utilizes the secret sharing technique to assign a share of $K_{mn}$ to each $ID^j_{mn}$; that is, $ID^j_{mn}$ has the share $K^j_{mn}$.

An event occurs in cell $(m, n)$ and is detected by $s \geq t$ nodes. The lead node AP in cell $(m, n)$ chooses a random $\alpha \in Z_q^*$ and computes $\theta = e(W, W)^{\alpha}$ to be broadcast to the other detecting nodes. Upon receiving $\theta$, each detecting node $ID^j_{mn}$ endorses the report $\Lambda$ by computing $U^j_{mn} = K^j_{mn} \cdot h(\Lambda \parallel \theta)$. The node then sends to AP $U^j_{mn}$ encrypted and authenticated with the pairwise key shared with the AP. Once receiving $t$ or more such endorsements, AP would randomly select $t$ endorsers denoted by a set notation $\Omega$ which may include itself. AP would then calculate $U_{mn} = \sum_{\Omega \in \Omega} U^j_{mn} = K_{mn} h(\Lambda \parallel \theta)$ and $Y_{mn} = U_{mn} + \alpha W$. The final report is $\langle \Lambda, Y_{mn}, h(\Lambda \parallel \theta) \rangle$. Once deriving $U_{mn}$, AP verifies its authenticity by checking if equation $e(U_{mn}, W) = (v_{mn}^{(0)})^{-h(\Lambda \parallel \theta)}$ holds, where $v_{mn}^{(0)} = e(K_{mn}, W)$. If the check does not succeed, AP should proceed to verify each received $U^j_{mn}$ by checking if (1) holds. Consider the following:

$$e(U^j_{mn}, W) = \prod_{j=0}^{t-1} (v_{mn}^{(j)})^{(ID^j_{mn} h(\Lambda \parallel \theta))} .$$

If the check succeeds, AP considers node $ID^j_{mn}$ legitimate. AP is therefore able to pinpoint all the endorsers offering false signatures and delete them from $\Omega$.

AP then sends to the sink the final report along a multihop path discovered using a secure multipath routing protocol. Upon receiving a report $\langle \Lambda, Y_{mn}, h(\Lambda \parallel \theta) \rangle$ to be forwarded, each intermediate node computes

$$\theta' = e(Y_{mn}, W) e(H(m \parallel n), -W_{pub})^{h(\Lambda \parallel \theta)} ,$$

where $W_{pub} = k^W$ is a public system parameter. If the report is authentic, then $\theta' = \theta$. Therefore, if $h(\Lambda \parallel \theta') = h(\Lambda \parallel \theta)$, then an intermediate node would consider the report authentic and hence forward it to the next hop.

However, LTE is not always feasible because it requires that every sensor node be equipped with localization capability, which incurs extra communication overhead as well as latency. Moreover, the bilinear pairing utilized in LTE is too expensive for low energy sensor nodes. In LTE, a data report must be consigned by $t$ out of $T$ nodes ($t \leq T$) in the event area. Thus, an adversary needs to compromise at least $t$ nodes in order to inject false data. It is worth mentioning, however, that the relationship between $t$ and $T$ is not fully discussed in LTE with respect to dealing with report disruption attacks. From our analysis, we have found that the critical relationship $T - t \geq t$, that is, the maximum
Table 1: Analysis of limitations.

| Schemes | Key-sharing limitation | T-threshold limitation | Node location limitation | Static route limitation | Lack of tolerance to FEDoS attacks | Lack of tolerance to PDoS attacks |
|---------|------------------------|------------------------|-------------------------|------------------------|-----------------------------------|---------------------------------|
| SEF     | Yes                    | Yes                    | No                      | No                     | Yes                               | Yes                             |
| IHA     | Yes                    | Yes                    | No                      | Yes                    | Yes                               | Yes                             |
| DSF     | Yes                    | No                     | No                      | No                     | Yes                               | Yes                             |
| RAS     | Yes                    | No                     | No                      | No                     | Yes                               | Yes                             |
| KAEF    | Yes                    | No                     | No                      | No                     | Yes                               | Yes                             |
| STEF    | Yes                    | No                     | Yes                     | Yes                    | Yes                               | Yes                             |
| PCREEF  | Yes                    | No                     | No                      | Yes                    | Yes                               | Yes                             |
| DEFS    | Yes                    | Yes                    | No                      | Yes                    | Yes                               | Yes                             |
| GPREF   | Yes                    | No                     | Yes                     | No                     | Yes                               | Yes                             |
| DREF    | Yes                    | No                     | No                      | No                     | No                                | No                              |
| EAB     | Yes                    | No                     | No                      | Yes                    | Yes                               | Yes                             |
| BECAN   | Yes                    | No                     | No                      | No                     | Yes                               | No                              |
| LBRSE   | Yes                    | No                     | Yes                     | Yes                    | Yes                               | Yes                             |
| LEDS    | Yes                    | No                     | Yes                     | Yes                    | No                                | No                              |
| CCEF    | Yes                    | No                     | Yes                     | Yes                    | Yes                               | Yes                             |
| PDF     | No                     | Yes                    | No                      | Yes                    | Yes                               | Yes                             |
| LTE     | No                     | No                     | Yes                     | No                     | No                                | No                              |

number of compromised nodes, that is, $t-1$, for the scheme to tolerate false data injection attacks cannot cooperatively cause the report disruption attacks. Thus, we have $T \geq 2t - 1$.

3. The Proposed Scheme

In this section, we describe the proposed DAEF, a data authentication and en-route filtering scheme, that can be used to ensure the security of data collection and transmission from WSNs in the context of IoT. In applications to which DAEF can be applied, we assume that a group of sensor nodes are used to monitor an event. In the proposed DAEF, a group ID-based signature is introduced for each event report so that any intermediate node and any Internet user with the identity of the group lead node can easily verify the event report, which easily removes the key-sharing and the $T$-threshold limitations, while realizing $T$-authentication to tolerate node compromise attacks without requiring static route and node localization technology. DAEF also employs the verifiable secret sharing algorithm to distribute and verify signature shares in order to defend against report disruption attacks. Last, but not the least, we employ the most efficient ID-based signature algorithm in DAEF to reduce computation overhead that results from signature generation and verification operations. Moreover, a multi-path routing protocol should be used in DAEF to resist selective forwarding attacks.

3.1. Assumptions. We assume that all the sensor nodes in WSNs are deployed uniformly and bootstrapped securely using the scheme proposed in [25] so that the one-hop neighboring sensor nodes can establish pairwise keys and trust relationships to form a network with multi-hop cluster-tree hierarchical topology. Each node establishes and stores a neighbor trust list as shown in Figure 2. We also assume that every event of interest can be detected by multiple, say $T$ ($T > 1$), sensor nodes in one group, each group covering a detecting area. Then, the event needs to be reported during which a group of at least $t$ ($T \geq 2t - 1$) nearby legitimate nodes should collaboratively agree on the event that will be forwarded to one or more Internet users. In this scenario, $T$ and $t$ are predefined system parameters and are determined by the application requirements. For each group, a lead head is elected and is responsible for collecting and summarizing all the received detection results from detecting nodes in the group, and generating a final report on behalf of the group. This group of neighboring nodes generates and broadcasts the signed report to a lead node which then aggregates the signatures before sending them to one or more Internet users through one or more forwarding nodes.

Moreover, we assume that the Internet users are determined by the service provider (SP) based on the service provided by the sensor nodes. Take the smart home applications as an example, the detection of fire in a home should be reported to the family members, security guards of the community, and the fire department, while the temperature in the home may be reported to all family members every two hours. The corresponding software code can be preloaded in the sensor nodes prior to deployment. Furthermore, the code can be dynamically updated by using an end-to-end secure communication protocol (referring to [26]).

3.2. Threat Model and Design Goals. An adversary can eavesdrop on all traffic, inject packets, replay older packets, and take full control of the compromised nodes to launch false report injection attacks and DoS attacks. In our model, we assume that most $T$-$t$ neighboring nodes in an event area
can be compromised. Our objective is to design a scheme to detect these attacks for the event report in the IoT scenario. DAEF should achieve the following goals.

1. It should not require the establishment of preshared keys between Internet users and sensor nodes (to overcome the key-sharing limitation).
2. It should not depend on the localization technology to prevent compromised nodes from breaking the whole WSN (to overcome the T-threshold limitation).
3. It should tolerate node compromises in the WSNs even if the locations of the sensor nodes may not be known (to overcome the node location limitation).
4. It can mitigate the impact of DoS attacks including report disruption attacks and selective forwarding attacks (to overcome the FEDoS and PDOs attacks).
5. It should keep the overhead of communication and computation as low as possible in the WSNs.

3.3. Preliminaries

3.3.1. ID-Based Signature. As discussed above, ECC-based signature (i.e., ECDSA) requires one point multiplication operation to generate a signature and two point multiplication operations to verify a signature. Moreover, authentication of the public key of the signer also requires two point multiplication operations to generate a signature and two point multiplication operations to verify the signature. For an ECC of 160 bites, ECDSA requires one point multiplication operation (i.e., ECDSA) requires one point multiplication operation to verify the signature with the length of a signature being 83 bytes. Let us briefly describe the vBNN scheme below.

Given a sensor node $ID_i$, the SP picks a random number $r_i \in Z_q$, where the multiplicative group $Z_q = \{1, \ldots, q - 1\}$ computes $R_i = r_iP$, where $P$ is a large prime, and an elliptic curve $E(F_p)$ is defined over a finite field $F_p = \{1, 2, \ldots, P - 1\}$. Then, SP calculates $S_i = r_i + xH_1(ID_i \parallel R_i)$ in which $x$ is the master key of the WSN picked by SP and $H_1 : \{0, 1\}^* \times G_2 \rightarrow Z_q$, where $G_2$ is an additive group of the prime order $q$, $R_i$ and $S_i$ are stored in the sensor node $ID_i$.

Given a message $M$, the signer $ID_i$ performs the following steps to sign the message.

1. Choose a random number $y \in Z_q$, and compute $Y = yP$.
2. Compute $h = H_2(ID_i \parallel M \parallel R_i \parallel Y)$ and $z = y + S_i h$, where $H_2 : \{0, 1\}^* \rightarrow Z_q$.
3. $(R_i, h, z)$ is the digital signature.

The signer then sends $(M, R_i, h, z)$ to the receiver. To verify the message and the signature, the receiver does the following steps.

1. Compute $c = H_1(ID_i \parallel R_i)$.
2. Check the equation $h = H_1(ID_i \parallel R_i \parallel M \parallel zP - h(R_i + cP_{pub}))$, where $P_{pub} = xP$ is a public parameter.

3.3.2. Verifiable Secret Sharing. Sensor node $ID_i$ generates a secret polynomial $f_S(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$, where $a_0, \ldots, a_{t-1}$ are random numbers picked by the sensor node $ID_i$ and the secret key $S_i$ can be picked as $S_i = a_0$. The secret share of $S_i$ for the neighboring node $ID_j$ is thus $C_j^i = f_S(ID_j)$. Then, any $t$ sensor nodes together can reconstruct $S_i$ by using Lagrange interpolation $S_i = \sum_{j=1}^t C_j^i \cdot \epsilon_j$, where $\epsilon_j = \prod_{k=1,k \neq j}^{t} (ID_j \parallel (ID_k - ID_j))$ is the Lagrange coefficient. However, it is computationally infeasible if fewer than $t$ sensor nodes try to reconstruct the secret key $S_i$. All $C_j^i$ must be distributed through the secure communication channels. The sensor node $ID_i$ broadcasts $\epsilon_0 = g^{th_n}$ and $\epsilon_n = g^{th_n}(mod p)$ ($n = 1, 2, \ldots, t - 1$), and every $ID_j$ can verify the received $C_j^i$ by using the equation $g^{C_j^i} = \prod_{k=0}^{t-1} g^{f_S(ID_k) \parallel (ID_k - ID_j)} (mod p)$, while $ID_i$ can verify the reconstructed $S_i$ by using the equation $g^{S_i} = \epsilon_0$.

3.4. The Data Authentication and Filtering Scheme

3.4.1. Initialization. During the bootstrapping phase, the lead node in every group distributes the secret share of $S_i$ to all group nodes. Specifically, in $i$th group, the lead node $ID_i$ generates a secret polynomial $f_S(x)$ and distributes the secret share $f_S(ID_j)$ to every group node $ID_j$ using the shared key between them. Then, $ID_i$ deletes $S_i$ and $f_S(x)$ but stores $f_S(ID_i)$. Therefore, $ID_i$ only needs to be authenticated by any other $t - 1$ group nodes and get $t - 1$ secret shares in order to reconstruct $S_i$.

3.4.2. Report Generation. When an event occurs, the lead node will prepare a report, say $E$. To get an agreement on the event from other group nodes, the lead node $ID_i$ broadcasts $E$ to all the group nodes and authenticates itself to them. After receiving $E$, a group node will find the difference between the received $E$ and what it has sensed. If the difference is
within a predefined error range, it will agree on $E$ and endorse the signature. These $T$ group members including $ID_j$ itself, taking one node $ID_k$ as an example, will generate one random polynomial $f_{y_j}^l(x)$ as shown in (3), in which the share of the random number is $C_{y_j}^l(k) = f_{y_j}^l(ID_k)$ ($k = 1, 2, \ldots, T$), distribute $C_{y_j}^l(k)$ to the other sensor nodes $ID_k$, and broadcast $e_j = g^{f_{y_j}^l(mod\; p)} (n = 0, 1, 2, \ldots, t - 1)$. Consider the following:

$$f_{y_j}^l(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}. \quad (3)$$

Note that the distribution of secret shares should be protected using the shared keys between the communicating peers. Therefore, each node will receive no less than $m-1$ ($t \leq m \leq T$) secret shares which should be verified as discussed in Section 3.3.2. For example, $ID_k$ should verify $C_{y_j}^l(k)$ received from $ID_j$ according to formula (4). Consider the following:

$$g^{C_{y_j}^l(k)} = \prod_{n=0}^{t-1} e_j(ID_k). \quad (4)$$

During the verification phase, a compromised group member may be detected. If $ID_j$ find a corrupted partial secret share sent by a group member, $ID_k$ broadcasts the ID of the compromised group member. If more than $t$ members claim that one node has been compromised, each legitimate sensor node can find all compromised group members and no less than $t$ legitimate group members. These $m$ legitimate sensor nodes should use the verified $m-1$ secret shares and its own share to compute the share of $y_j$, denoted as $y_j^l$, shown in (5). Consider the following:

$$y_j^l = \sum_{n=1}^{m} f_{y_j}^n(ID_j)$$

$$= \left( \sum_{n=1}^{m} a_0 \right) + \left( \sum_{n=1}^{m} a_1 \right) ID_j + \left( \sum_{n=1}^{m} a_2 \right) ID_j^2 + \ldots + \left( \sum_{n=1}^{m} a_{t-1} \right) ID_j^{t-1}. \quad (5)$$

The secret random number $y_j$ is generated from the polynomial $f_{y_j}(x) = \sum_{n=1}^{m} f_{y_j}^n(x)$, shown in formula (6), which is endorsed by these $m$ legitimate sensor nodes and $y_j = f_{y_j}(0)$. Therefore, no sensor node knows $y_j$, and any $t$ sensor nodes can reconstruct $y_j$ using Lagrange interpolation: $y_j = \sum_{j=1}^{m} l_j y_j^l$, in which $l_j = \prod_{n=1, n\neq j}^{m}(ID_n/(ID_n - ID_j))$. Consider

$$f_{y_j}(x) = \sum_{n=1}^{m} f_{y_j}^n(x)$$

$$= \left( \sum_{n=1}^{m} a_0 \right) + \left( \sum_{n=1}^{m} a_1 \right) x + \left( \sum_{n=1}^{m} a_2 \right) x^2 + \ldots + \left( \sum_{n=1}^{m} a_{t-1} \right) x^{t-1}. \quad (6)$$

Each legitimate neighboring node $ID_j$ except the lead node $ID_j$ sends $l_j y_j^l P$ to $ID_j$, which then sums up the received $m$ shares to get $Y_j = \sum_{j=1}^{m} l_j y_j^l P$ and broadcasts $Y_j$ along with $R_i$. Each legitimate neighboring node $ID_k$ including the lead node $ID_k$ computes $z_j = l_j y_j^l + l_j C_{y_j}^l h$, where $h = H_2(ID_j \parallel E \parallel R_i \parallel Y_j)$ and sends $z_j$ to $ID_j$ which then sums up $z$ (7). It is possible that some of the neighboring nodes have been compromised during this phase and, thus, may provide the lead node $ID_j$ with incorrect signatures. Therefore, $ID_i$ should verify their authenticity by checking the equation $Y_j = zP - h(R_i + c P_{pub})$ where $c = H_2(ID_j \parallel R_i)$ Consider the following:

$$z = \sum_{j=1}^{m} (l_j y_j^l + l_j C_{y_j}^l h) = \sum_{j=1}^{m} l_j y_j^l + \sum_{j=1}^{m} l_j C_{y_j}^l h = y_i + S_i h. \quad (7)$$

Finally, $ID_j$ broadcasts the final data report $(E, R_i, h, z)$ and assigns multiple upstream nodes in its neighbor trust list to make the report forwarded to the Internet users through multipath routing. In the cases in which the compromised lead node may either not send the final report or transmit a bogus report with a wrong $(E, R_i, h, z)$, it will be detected by all legitimate group nodes. The verification is the same as the en-route filtering operations to be described in Section 3.4.3. In this case, the legitimate neighboring nodes will randomly elect a new lead node among themselves to generate a new threshold-endorsement and send the final report to the Internet users. The whole report generation procedure is illustrated in Algorithm 1.

### 3.4.3. En-Route Filtering of Data Report. We denote $P_f$ as the en-route verification probability. The forwarding sensor node verifies the signature of a report with the probability $P_f$ which is a predefined system parameter. As discussed in Section 3.3.1, the verifying intermediate node or the final Internet user first computes $c = H_2(ID_j \parallel R_i)$, then checks (8). The data report will be regarded as authentic and forwarded to multiple upstream nodes in their neighbor trust lists if the verification is successful, otherwise, it will be immediately discarded. Consider

$$h = H_2(ID_j \parallel R_i \parallel E \parallel zP - h(R_i + c P_{pub})) \quad (8)$$

### 4. Analysis

#### 4.1. Security Analysis

4.1.1. Resilience to Node Compromise Attacks. DAEF uses the threshold signature generation to sign any event report. The attacker must know the private key $S_i$ and the secret random number $y_i$ to forge the signature of $ID_i$ by compromising at least $t$ nodes in the event area. In some cases, the lead node itself may have been compromised, resulting in a higher level of risk. However, DAEF does not reveal any $C_{y_j}^l$ and $y_j^l$ at any step. Firstly, the initialization phase is secure in which the lead node distributes the shares of $S_i$ within a short time after bootstrapping. Secondly, each neighboring node submits
4.1.2. Mitigation of Report Disruption Attacks. DAEF affects any other groups. In the report generation phase, at least $y_1$ sensor nodes cooperatively generate the secret random $\frac{y_1}{n}$. In the report generation phase, at least one of the neighboring nodes, which may be disrupted by compromised nodes. For example, $z_j = l_j y_j^I + l_j C_j^I h$ that is submitted by each neighboring node has two unknown numbers $y_j^I$ and $C_j^I$, so the lead node cannot derive $y_j^I$ and $C_j^I$. Finally, should the lead node change the report with a wrong $(E, R_i, h, z)$ in the final step, it would be detected by the forwarding nodes as well as by all the legitimate neighboring nodes. These nodes can then select a new lead node to generate a new threshold-endorsement and send the final report to the intermediate nodes. In the worst case, even if the attacker can derive the private key $S_i$ by compromising $t$ nodes in the event area, it will not affect any other groups.

4.1.2. Mitigation of Report Disruption Attacks. DAEF leverages verifiable Shamir’s secret sharing cryptography described in Section 3.3.2 which has been shown to be secure [28]. In the report generation phase, at least $t$ legitimate sensor nodes cooperatively generate the secret random number $y_i$ by exchanging the shares $C_j^I (k) = f_j^I (ID_j)$, which may be disrupted by compromised nodes. For example, an attacker may provide an incorrect share $C_j^I (k)$ to a neighboring node so that it will not get the right share $y_j^I = \sum_{k=1}^{m} f_j^I (ID_j)$. However, in DAEF, each node will verify the received shares, detect compromised neighboring nodes, and broadcast the detection result so that only legitimate shares will be used in the $y_j^I$ and only the shares $z_j$ computed by legitimate neighboring nodes can be used by the lead node. Note, however, that if the attacker only distributes the wrong shares to only some of the legitimate neighboring nodes that are able to detect the wrong shares, based on the detected results broadcast by such neighboring nodes, it is not possible for the legitimate neighboring nodes to identify the compromised nodes.

4.1.3. Mitigation of Selective Forwarding Attacks. In DAEF, in order to mitigate selective forwarding attacks, the lead node and the intermediate nodes would forward the final report $(E, R_i, h, z)$ to multiple upstream nodes that are in their neighbor trust lists to ensure that the report is forwarded to the Internet users through multipath routing. Unless all the forwarding nodes are compromised, the legitimate report will ultimately be delivered to the destinations. However, this solution will incur high communication overhead. In the worst case in which all the upstream nodes of a forwarding node are compromised, another route path should be used by using a secure multi-path routing protocol in the WSN, such as SPREAD [29], which is out of the scope of this paper.

4.2. Performance Analysis. In this section, we evaluate the performance of DAEF in terms of filtering efficiency, the number of hops that false data can travel, and the ratio of compromised area, which are the main metrics for the evaluation of en-routing filtering schemes [30]. We also analyze and compare DAEF to LTE in terms of computation, communication, and energy consumption. We conducted all experiments in the analysis, evaluation, and comparison by using MATLAB [31] plus some programming in VC++ whenever necessary.

4.2.1. General Analysis. First, let us analyze filtering efficiency $P_h$ which is defined as the probability of successful filtering of false data within a specified number of hops. Similar to LTE, the probability of false data that can be filtered out within $h$ hops is

$$P_h = 1 - \left(1 - P_f \right)^h.$$  

(9)

Clearly, the greater the value of $P_f$, the greater the $P_h$ can achieve, that is, the better the filtering efficiency. However, a smaller $P_f$ can lower the computation overhead of intermediate nodes. Figure 3 shows the filtering efficiency with different $P_f$ from which we can see that when $P_f$ is 0.5, more than 90% of false reports can be filtering out within 4 hops. For a small $P_f$, say 0.2, less than 11% of false reports can travel over 10 hops. Therefore, for a large WSN which has long

\[
\begin{align*}
\text{Algorithm 1: Report generation procedure.}
\end{align*}
\]

\[
\begin{align*}
\text{for (each sensor } ID_j, j = 1, 2, \ldots, T) \\
ID_j; C_j^I (k) = f_j^I (ID_j) (k = 1, 2, \ldots, T) \\
ID_j \rightarrow \text{ID}_k; C_j^I (k) \\
ID_j \rightarrow \ast; \varepsilon_{x_k} = g^{\alpha_k} (\text{mod } p) (n = 0, 1, 2, \ldots, t - 1) \\
\text{for (each sensor } ID_j, j = 1, 2, \ldots, T) \\
ID_j; g^{C_j^I (k)} = \prod_{j=0}^{t-1} g^{x_k} (\text{mod } p) \\
ID_j; y_j^I = \sum_{m=1}^{m} f_j^I (ID_j) \\
ID_j \rightarrow \text{ID}_j; l_j y_j^I P \\
ID_j \rightarrow \ast; Y_i = \sum_{j=1}^{m} l_j y_j^I P, R_i \\
\text{for (each sensor } ID_j, j = 1, 2, \ldots, m) \\
ID_j \rightarrow \text{ID}_j; z_j = l_j y_j^I + l_j C_j^I h \\
ID_j \rightarrow \ast; (E, R_i, h, z)
\end{align*}
\]
forwarding paths, DAEF can efficiently filter out false reports as early as possible to save the energy of legitimate nodes.

The number of hops that false data can travel \( E(h) \) is defined as the average hops that false data are forwarded before being filtered and dropped, which reflects the filtering effectiveness. Similar to LTE, the average number of hops that a false report is forwarded before being filtered out is

\[
E(h) = \sum_{i=1}^{\infty} i P_f (1 - P_f)^{i-1} = \frac{1}{P_f}. \tag{10}
\]

The ratio of compromised area \( P_s \) is defined as the percentage of compromised sensor nodes in the terrain, which reflects the effectiveness of filtering resilience to the increase on the number of compromised nodes. Given that the network size is \( N \) and that the average number of nodes in each group is \( T \), when the attacker successfully compromises \( Nc \) sensor nodes, the probability that no node in an event group is compromised is

\[
P(0) = \frac{C_{Nc}^{\frac{T}{Nc} - T}}{C_{Nc}^{Nc}}. \tag{11}
\]

Let \( P(0) \) represent the probability that \( i \) nodes are compromised in a group. Then,

\[
P(i) = \frac{C_{T}^{i} C_{Nc}^{Nc-i}}{C_{Nc}^{Nc}}. \tag{12}
\]

Therefore, the percentage of compromised nodes is

\[
P_s = 1 - \sum_{i=0}^{T-1} P(i) = 1 - P(0) - \sum_{i=1}^{T-1} \frac{C_{T}^{i} C_{Nc}^{Nc-i}}{C_{Nc}^{Nc}}. \tag{13}
\]

Figure 4 shows the resilience as the number of compromised nodes increases. We can observe that the percentage of compromised groups increases very slowly with an increasing number of compromised nodes when less than 20% of all the nodes are compromised. Even if the number of compromised nodes reaches 200, only 10% of groups are compromised in all the cases except \( (t, T) = (3, 11) \) and \( (t, T) = (4, 11) \).

4.2.2. Comparison Analysis. We analyze DAEF and LTE in terms of computation cost and communication overhead and then compare them in terms of energy consumption to show the advantages that DAEF has over LTE.

First, we perform the analysis on computation cost. In all the schemes, expensive operations are normally pairing \((P_a)\), point multiplication \((P_m)\), and exponentiation \((\text{Exp})\). In DAEF, each endorsing sensor node needs to do one point multiplication operation to generate \( l_j y_j P \) and \( T \times t \) exponentiation operations which include \( t \) exponentiation operations to generate \( \epsilon_n \) \((n = 0, 1, 2, \ldots, t-1)\) and \( (T-1) \times t \) exponentiation operations to verify \( T - 1 \) received shares. Thus, the total number of computational operations in an event group is \( T \times P_m + T^2 t \times \text{Exp} \). Meanwhile, each verifying forwarding sensor node needs three point multiplication operations to authenticate an event report. In contrast, in LTE, the number of computational operations in an event group is \( 2 \times P_a + (T + 1) \times P_m + 2 \times \text{Exp} \) in cases in which no compromised nodes are selected by the lead node but is \( (T + 1) \times P_a + (T + 1) \times P_m + (Tt - t + 2) \times \text{Exp} \) in the worst case. In addition, each forwarding sensor node needs two pairing operations and one exponentiation operation to authenticate an event report.

For communication overhead, which is defined as the total number of messages generated in an event group, in DAEF, the \( T \) sensor nodes have to jointly generate a random number \( y_i \) for each report, which contributes most to the
communication overhead because the private key $S_i$ can be distributed during the bootstrapping phase. For a share $y_j$, each sensor node needs to send $T - 1$ secret shares to the $T - 1$ neighboring nodes and broadcast one promise $e_n$, $(n = 0, 1, 2, \ldots, t - 1)$ and one detection result. In the signature generation phase, each legitimate group sensor node sends $l_j y_j P$ and $z_j$ to the lead node and the lead node broadcasts $Y_j$ along with $R_i$. Thus, the total number of messages required to generate a signature for an event report is $(T + t + 1)T$. In contrast, in LTE, each endorsing node only needs to send one share $U^t_{mn}$ to the lead node which should broadcast $\theta$. Thus, the total number of messages required to generate a signature for an event report is $T$.

Note that in the above analysis, we assume that there is no compromised node in any of the event groups. Let us now analyze and compare DAEF to LTE in terms of energy consumption for the whole WSN under the assumption that there is at least one compromised node in an event group at the time of reporting an event, for these two schemes offer a similar level of security and both can deal with report disruption attacks and selective forwarding attacks.

We employ the similar model to LTE when performing analysis and comparison on energy consumption which is determined by communication overhead as well as computation cost. We assume that the sensor nodes have the same capabilities as those of a standard Crossbow’s MICA2 mote [32] which has 8-bit ATmega128L clocked at about 7.37 MHz microcontroller and complies with the IEEE 802.15.4 standards with data transmission rate of 12.4 kbps. According to [4], completing a 160-bit point multiplication operation of ECC, a pairing operation, and an exponentiation operation consumes 24.3 mJ, 62.73 mJ and 2.81 mJ, respectively. In addition, MICA2 consumes 52.2 $\mu$J, and 19.4 $\mu$J to transmit and to receive one byte, respectively. We assume that the length of the node’s ID is 2 bytes, making the lengths of $C_{y_i}(k)$, $e_n$, $l_j y_j P$, $z_j$, $Y_j$ and $R_i$ to be $2t$ bytes, $2t$ bytes, $40$ bytes, $20$ bytes, $40$ bytes, and $40$ bytes, respectively. The original report is assumed to be 15 bytes, thus allowing us to transmit a report in one data packet. We denote $e$ as the average number of hops a report travels in the WSNs. For the sake of simplicity, we only consider the single routing path; thus, both schemes involve $e P_j$ en-route filtering operations.

In the analysis, we specify $(t, T)$ to be $(2, 3), (3, 5), (4, 7), (5, 9)$, and $(6, 11)$, respectively, because of the relationship between $t$ and $T$ discussed in Section 2.4. Figure 5 shows the energy consumption for various $e$ when $P_j = 0.2$ under the condition that the number of compromised nodes in the event group is the maximum value $t - 1$. We can see from the figure that energy consumption in DAEF is lower than that in LTE for $(2, 3), (3, 5), (4, 7)$, and $(5, 9)$. However, the difference narrows as the value of $T$ increases until when $(t, T)$ is larger than $(6, 11)$ where DAEF will consume more energy than LTE. In addition, when $e$ increases by one hop, the increase in energy consumption in DAEF is about 15 mJ whereas that in LTE is more than 25 mJ. That is because the energy consumption of computation in DAEF that incurs $O(n)$ cost of point multiplication and $O(T^2 T)$ cost of exponentiation for report generation and three point multiplication operations for report en-route verification is lower than that in LTE that incurs $O(T)$ cost of pairing and $O(t)$ cost of point multiplication as well as $O(tT)$ cost of exponentiation for report generation and two pairing operations and one exponentiation operation for report en-route verification. However, the energy consumption of communication in DAEF for generating $O(t^2, T)$ communication cost is higher than that in LTE which only generates $O(t, T)$ communication cost.

Figure 6 shows the energy consumption for various $P_j$ when $e = 10$ under the condition that the number of compromised nodes in the event group is the maximum value $t - 1$. With the same $(t, T)$, the difference in energy consumption gets higher as $P_j$ increases. This is because one filtering operation requires two pairings and one exponentiation in LTE which incurs more cost of computation, about $128$ mJ, than three point multiplications, about 72 mJ, of one filtering operation in DAEF.

Figure 7 shows the energy consumption as the number of compromised nodes increases in an event group when $P_j = 0.2$ and $e = 10$. We can see from the figure that both DAEF and LTE perform better as the number of compromised nodes increases with the same $(t, T)$. This is because the number of legitimate nodes will decrease as the number of compromised nodes increases, hence reducing the computation cost and communication overhead in both schemes. Meanwhile, in DAEF, the larger the value of $T$ is, the larger the difference is for the same $(t, T)$. In LTE, however, the reduction in energy consumption becomes less significant as the value of $T$ increases. That is because the change in the communication overhead in DAEF is more than that in LTE in terms of the number of compromised nodes, which can be seen when $(t, T) = (5, 9)$.

Figure 8 shows the energy consumption for various parameter $t$ when $P_j = 0.2$ and $e = 10$ under the condition that the number of compromised nodes in the event group is maximum value $t - 1$. The energy consumption in DAEF is lower than that in LTE except for the values $T \geq 11$ and $t > 4$. However, the former increases slowly while the latter decreases as $t$ increases. In LTE, regardless of the value of $t$, the computation cost has little difference, which results from the number of valid shares $U^t_{mn}$ randomly selected by the lead node. Moreover, the larger value of $t$, the more effective computation and communication get, which reduces the waste of energy. In DAEF, the slowly increasing energy consumption results from the computation and broadcasting of promise $e_n$, $(n = 0, 1, 2, \ldots, t - 1)$.

In conclusion, DAEF outperforms LTE for data authentication and en-route filtering when an event group has a smaller number of nodes and larger number of compromised nodes.

5. Conclusion

In this paper, we proposed DAEF, a new data authentication and filtering scheme, to ensure the security of data collection and transmission from WSNs in the context of IoT. In the scheme, the verifiable secret sharing cryptography is used for the distribution of the shares to multiple
neighboring collective sensor nodes based on the most efficient ID-based signature scheme. As long as an adversary does not compromise more than $T-t$ neighboring nodes in an event area, any event report can be collectively generated with a digital signature attached and forwarded via multipath routing to multiple Internet nodes. Analysis on the proposed scheme showed that DAEF can effectively defend against node compromised attacks and DoS attacks in the forms of report disruption attacks and selective forwarding attacks. Quantitative analysis to compare DAEF to the LTE scheme has also been performed in terms of energy consumption in which we showed that DAEF outperforms LTE in terms of energy consumption when fewer numbers of nodes and more numbers of compromised nodes of a group exist in the event group. In the future, we will conduct more experiment in real network settings to verify the results and to further improve the performance in terms of latency in DAEF.
Acknowledgments

The work in this paper has been supported by funding from National Natural Science Foundation of China (61272500) and from Beijing Education Commission Science and Technology Fund (KM2010010005027).

References

[1] N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals,” IETF RFC 4919, Internet Engineering Task Force, 2007.

[2] G. Montenegro, N. Kushalnagar, and J. Hui, “Transmission of IPv6 packets over IEEE 802.15.4 networks,” IETF RFC 4944, Internet Engineering Task Force, 2007.

[3] L. B. Oliveira, A. Kansal, C. P. L. Gouvêa et al., “Secure-TWS: authenticating node to multi-user communication in shared sensor networks,” The Computer Journal, vol. 55, no. 4, pp. 384–396, 2012.

[4] R. Yasin, E. Ritter, and G. Wang, “An authentication framework for wireless sensor networks using identity-based signatures,” in Proceedings of the 10th IEEE International Conference on Computer and Information Technology (CIT ’10), pp. 882–889, Bradford, West Yorkshire, UK, July 2010.

[5] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” in Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’04), pp. 2446–2457, Hong Kong, China, March 2004.

[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 259–271, Oakland, Calif, USA, May 2004.

[7] Q. Sun and M. Wu, “A double key-sharing based false data filtering scheme in wireless sensor networks,” in Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom ’11), 8th IEEE International Conference on Embedded Software and Systems (ICESS ’11), 6th International Conference on Frontier of Computer Science and Technology (FCST ’11), pp. 509–516, Changsha, China, November 2011.

[8] Y. Hu, Y. Lin, Y. Liu, and W. Zeng, “RAS: a robust authentication scheme for filtering false data in wireless sensor networks,” in Proceedings of the 15th IEEE International Conference on Networks (ICON ’07), pp. 200–205, Adelaide, Australia, November 2007.

[9] T. Yuan, S. Zhang, Y. Zhong, and J. Ma, “KAEF: an en-route scheme of filtering false data in wireless sensor networks,” in Proceedings of the IEEE International Performance Computing and Communications Conference (IPCCC ’08), pp. 193–200, December 2008.

[10] C. Krauß, M. Schneider, K. Bayarou, and C. Eckert, “STEF: a secure ticket-based en-route filtering scheme for wireless sensor networks,” in Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES ’07), pp. 310–317, Vienna, Austria, April 2007.

[11] X. Yang, J. Lin, P. Moulema, W. Yu, X. Fu, and W. Zhao, “A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems,” in Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, pp. 92–101, Macau, China, 2012.

[12] Z. Yu and Y. Guan, “A dynamic en-route filtering scheme for data reporting in wireless sensor networks,” IEEE/ACM Transactions on Networking, vol. 18, no. 1, pp. 150–163, 2010.

[13] L. Yu and J. Li, “Grouping-based resilient statistical en-route filtering for sensor networks,” in Proceedings of the 28th Conference on Computer Communications (INFOCOM ’09), pp. 1782–1790, Rio de Janeiro, Brazil, April 2009.

[14] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “Poster abstract: a dos-resilient en-route filtering scheme for sensor networks,” in Proceedings of the 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’09), pp. 334–344, New Orleans, La, USA, May 2009.

[15] Y.-S. Chen and C.-L. Lei, “Filtering false messages en-route in wireless multi-hop networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’10), pp. 1–6, Sydney, Australia, April 2010.

[16] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, “BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 1, pp. 32–43, 2012.

[17] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward resilient security in wireless sensor networks,” in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC ’05), pp. 34–45, Chicago, Ill, USA, May 2005.

[18] K. Ren, W. Lou, and Y. Zhang, “LEDS: providing location-aware end-to-end data security in wireless sensor networks,” in Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM ’06), pp. 1–12, Barcelona, Spain, April 2006.

[19] H. Yang and S. Lu, “Commutative cipher based en-route filtering in wireless sensor networks,” in Proceedings of the IEEE 60th Vehicular Technology Conference: Wireless Technologies for Global Security, pp. 1223–1227, Los Angeles, Calif, USA, September 2004.

[20] H. Wang and Q. Li, “Achieving robust message authentication in sensor networks: a public-key based approach,” Wireless Networks, vol. 16, no. 4, pp. 999–1009, 2010.

[21] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “A constrained function based message authentication scheme for sensor networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’09), pp. 1–6, Budapest, Hungary, April 2009.

[22] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location-based compromise-tolerant security mechanisms for wireless sensor networks,” IEEE journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247–260, 2006.

[23] C. Krauß, M. Schneider, and C. Eckert, “Defending against false-endorsement-based DoS attacks in wireless sensor networks,” in Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec ’08), pp. 13–23, New York, NY, USA, April 2008.

[24] J. Deng, R. Han, and S. Mishra, “Defending against path-based dos attacks in wireless sensor networks,” in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’05), pp. 89–96, Alexandria, Va, USA, November 2005.

[25] H. Yu and J. He, “Trust-based mutual authentication for bootstrapping in 6LoWPAN,” Journal of Communications, vol. 7, no. 8, pp. 634–642, 2012.
[26] H. Yu, J. He, T. Zhang, P. Xiao, and Y. Zhang, “Enabling end-to-end secure communication between wireless sensor networks and the internet,” World Wide Web, vol. 16, no. 4, pp. 515–540, 2013.

[27] X. Cao, W. Kou, X. Zeng, and L. Dang, “Identity-based anonymous remote authentication for value-added services in mobile networks,” IEEE Transactions on Vehicular Technology, vol. 58, no. 7, pp. 3508–3517, 2009.

[28] P. Feldman, “A practical scheme for non-interactive verifiable secret sharing,” in Proceedings of the 28th Annual Symposium on Foundations of Computer Science, pp. 427–438, 1987.

[29] W. Lou, W. Liu, and Y. Fang, “SPREAD: enhancing data confidentiality in mobile ad hoc networks,” in Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’04), pp. 2404–2413, Hong Kong, China, March 2004.

[30] J. Lin, X. Yang, W. Yu, and X. Fu, “Towards effective en-route filtering against injected false data in wireless sensor networks,” in Proceedings of the 2011 IEEE Global Telecommunications Conference, pp. 1–5, Houston, Tex, USA, December 2011.

[31] S. Chapra, Applied Numerical Methods W/MATLAB: For Engineers & Scientists, McGraw-Hill Science, New York, NY, USA, 3rd edition, 2011.

[32] Crossbow, “MICA2,” http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2Datasheet.pdf.