A Reliable Framework for Secure Communication and Health Assessment of Soldiers in the Battlefield

Maaz Bin Ahmad¹, Muhammad Asif², Khalid Masood², Mohammad A. Al Ghamdi³, Sultan H. Almotiri³, and Arfan Ali Nagra²

Abstract
Wars against the enemy are mandatory for the integrity of a nation. With the passage of time, the nature of war is being changed, to some extent from a conventional war to the network-centric warfare. The rate of soldiers death has increased in modern combat operations. The lack of secure connectivity and the health (mental and physical) of soldiers are among a few major reasons for the increased mortality. Mental health or stress level produces permanent changes in the physiological systems of a soldier and long-term diseases such as asthma, diabetes, and hypertension are activated with chronic stress. Although modern communication technologies may provide huge support in the efficient conduction of combat’s activities but it is at the cost of huge power consumption. The proposed research presents a computationally efficient and low-power framework that not only ensures secure communication but also provides a robust command and control system to monitor the mental stress, injury, and death of soldiers. In the suggested framework, the Advanced Encryption Standard (AES) is used for communication that is highly suitable for power constraint devices. A wearable sensor system is suggested that can be embedded in a soldier’s uniform to assist in the recording of real-time stress, injury, and death of soldiers. The system contains a heart-rate monitor to record variations in heartbeats, an EDA sensor for skin conductance, and a respiration sensor for respiration variations along with a holster unit for storage and transmission of biomedical signals. Furthermore, it also provides a mechanism to prevent misuse of soldiers’ communication equipment by the enemy thus ensuring more security. The experimental analysis shows that the proposed mental stress computation module achieved 83.33% accuracy. Moreover, a score-based comparison is performed with the existing techniques and it is found that the proposed mechanism outperformed its counterparts with 37.5% improvements in the features-based analysis. The flexibility, security, efficiency, and reliability of the framework make it appropriate for modern warfare scenarios.

Keywords
secure communication, battlefield, mental health assessment, mental stress, reliable transmission, AES

Introduction
Providing real-time error-free communication links among warriors has been an active area of research. Traditional wired communication networks are not only expensive but are also prone to error due to distance, topography of battlefield, weather, etc. However, modern wireless communication systems are easy to install, expandable and have potential to connect soldier-to-soldier in any ecological circumstances (Hutzell, 2017). The importance of wireless communication has become evident in the First World War, when it played a decisive role in the heat of battlefield. Therefore, optimum wireless communication network, navigation system and coordination among the soldiers are crucial for success.

¹Karachi Institute of Economics and Technology, Pakistan
²Lahore Garrison University, Pakistan
³Umm Al-Qura University, Makkah City, Saudi Arabia

Corresponding Author:
Maaz Bin Ahmad, COCIS, Karachi Institute of Economics and Technology, Korangi Creek, 75190, Karachi, Pakistan.
Email: maaz@kiet.edu.pk
in the combat activities (Abirami et al., 2017; Cotton et al., 2009; Gondalia et al., 2018; Govindaraj & Banu, 2013; Jee et al., 2017; Nikam et al., 2013).

In the modern warfare, navigation systems are considered to be an essential part of the combat strategy and are used for better monitoring of the battlefield (Chhabra et al., 2017). Navigation can be provided using Global Positioning System (GPS) which helps the control room to determine the real-time location of soldiers (Gondalia et al., 2018). Navigation information can also be used to direct the soldiers to move to the desired location based upon combat's strategy. Real-time secure communication links between the troops and command & control center is a crucial part of the combat operation (Ali et al., 2018). Besides the advanced safety measures, a soldier with secure communication facility is now becoming a need for the modern combat operation. The concept of connected soldiers contains radios for communication, navigation, health monitoring, and video links etc.

To ensure the success of a mission and safety of the soldiers, real-time critical situational information must be shared (Radhappa et al., 2018). A soldier along with weapons can be equipped with various electronic equipment that includes helmet mounted camera, GPS receiver, voice communication system, and health monitoring system. The equipment assists the soldier in protecting his life, coordinating with other soldiers and communication with command and control center (Conti et al., 2018; Rahman & Tomar, 2018). Wireless network is an attracting option due to its mobility, scalability and easy installation nature. It performs better in a battlefield where soldiers are dispersed and are on the continuous move in any geographical terrain. Various modern equipment and sensors are interconnected through wireless network that can be helpful to analyze the remote location in a timely and consistent manner (Akyildiz et al., 2002; Saad et al., 2021).

For stress conditions in a battlefield, the body responds to factors that cause stress and it undergoes physical and psychological changes. The body releases hormones and cortisol to be prepared for the challenges that are forecasted by brain as dangerous. The physical changes in response to stress are similar to those changes when a person performs physical activities such as running and exercise. To differentiate between the two, a few baseline procedures are performed that record physical measures in a treadmill performance task. The modified physical measures are now in proportional to mental stress and determine various levels of stress. Brain signals, however, vary directly with stress and they do not need any baseline procedures. Various physical measures that respond to stress include heart rate variations, blood pressure, changes in respiration, pupil dilation, and skin wetness. These measures can be measured more efficiently than a few other physical variations such as voice changes, gesture variation, and face expressions. For a soldier, an embedded system can be designed that contains wearable sensors to record a few physical measures such as heart rate variations, respiration changes, and skin conductance. A wearable soldier cap is also proposed that contains electrodes to record brain signals. A holster unit is attached to the waist belt of soldiers to record and process signals from the four sensors namely heart rate monitor, EDA sensor for skin current, respiratory sensor, and EMG sensor for neural signals from the brain. It also contains lithium batteries that provide power to the unit for a couple of days. The standard protocol to induce stress comprises of various controlled activities and mental challenges.

This paper proposes a computationally efficient, secure, low power, and reliable framework communication and real-time sharing of tactical data among soldiers and to their command and control center. The impact of stress and depression can be determined using a proposed wearable sensor system that contains wireless sensors to capture biomedical signals representing various stress levels. Following are the main objectives and contributions of the proposed framework:

- To provide a flexible blueprint of the communication that can be used according to the war scenario and available technology.
- To provide secure and reliable communication.
- To determine mental stress and depression levels.
- To monitor real-time location and health status of the soldiers.
- To prevent misuse of soldier’s communication equipment by the enemy.

The rest of the paper is organized as follows: The “Literature review” presents the existing work and identifies its limitations. The section “Proposed framework” presents the suggested framework for secure communication and health assessment of soldiers in the battlefield. Experimental evaluation of different modules of the proposed framework is made in the “Experimental analysis” section. The section “Quantitative analysis and discussion” presents a score-based comparison of the proposed framework with existing techniques and discussion. Finally, the conclusion is made in “Conclusion” section.

Literature Review

Several efforts have been made by the researchers to monitor and assist battlefield scenarios. DeCleene et al. (2001) proposed a key management scheme for highly
mobile wireless network environment of battlefield where the nodes (soldiers) frequently join and leave the network. In order to provide forward and backward confidentiality, all nodes are re-keyed when a node joins or leaves the network. It also addresses the solution for key management among the different groups of troops (geographically located near or far) and multicast communication among these groups and control center. It uses a hierarchical structure in which a local key distributor at each level distributes key and coordinates with central key distributor. Central key distributor provides communication among the local key distributors. The proposed scheme is inefficient for small resource constraint devices (having limited battery power and computational resources) to perform frequent re-keying for securing the communication. Another drawback is that during the re-keying process, no communication is possible. So frequent re-keying is not acceptable during sophisticated combat operations.

Nemeroff et al. (2001) presented an infrastructure for communication among the sensors and to their control center in a Wireless Sensor Network (WSN) for battlefield at enemy areas. The sensors in WSN are deployed in enemy areas to detect targets. These sensors are interconnected in an ad hoc mode and they pass their data to intermediate nodes which perform relay operations. The intermediate nodes collect the data, aggregates and send it to the control center. For extending the range of a network, UAVs (Unmanned Aerial Vehicle) are also suggested for relaying data to control centers. Various aspects of a reliable and secure network remained unaddressed in the proposed scheme. The technology which is used for communication among the relaying nodes and UAVs is not defined. No mechanism for keeping the data confidential from nodes to control center is provided in the proposed research.

Durresi et al. (2008) proposed a scheme for secure data transfer from the stationery sensors network to the mobile receiving nodes. The mobile nodes are pre-configured with a few randomly selected keys along with identifiers from a key pool. The stationery nodes in the network are also configured with a few randomly selected keys. The numbers of keys configured in mobile nodes are greater than static node. The benefit of having less number of keys configured in stationery nodes is that fewer keys will be compromised if one or more static nodes are captured by enemy. When a mobile node wants to communicate with a particular static node, it broadcasts some identifiers from its key set. The static node will match the broadcasted key identifiers with its own key set. If a match is found, the static node will establish a session key for further communication. The session key can be reused later on for communication between the mobile and static node to reduce the overhead. This scheme has serious flaws. First, if enemy captures any static node, it can extract the keys and can establish a session key with mobile node without being detected. Secondly, establishing a session key with each mobile node is very resource intensive and infeasible for battery powered static nodes. Third, due to random key selection from Key Pool by both static and mobile nodes, the probability of sharing a key of mobile node with static node is reduced. To overcome this problem, author has assumed the high density of static nodes in the network. This high density of static nodes may lead to many problems such as high cost, difficult deployment, complex routing protocol and larger communication delay. The number of compromised keys can also be increased if more static nodes are captured by enemy due to their high density.

Watthanawisuth et al. (2011) emphasized on the usage of ZigBee technology for providing secure communication among soldiers in the battle field due to its various features such as scalability, low cost and easy installation. The scheme suggests the use of star, mesh, and tree topology for interconnecting the ZigBee nodes and transporting real time tactical data from nodes in battlefield to control center. The proposed scheme has many loop holes. From the perspective of security, it uses Personal Area Network (PAN) ID for authentication of the node that wants to join the network. The mechanism for secure distribution of PAN ID among the nodes is not defined. The Enemy can easily intercept the messages that are being exchanged among the nodes and can extract the PAN ID. The proposed scheme is also unreliable because it assumes mesh network for transporting the tactical data from battlefield to command and control center which is infeasible in reality.

Sze-Toh & Yow (2002) presented an architecture for monitoring the soldier’s vital symptoms and real time location in battlefield by the command and control center through Beidou system. Beidou is a satellite navigation system which provides real time location information (just like Global Positioning System (GPS)) in the whole territory of China. One of its dominating features is that it also provides two ways short messaging service between any two Beidou supported devices. The collection of real time vital symptoms can help in immediate identification of an injured soldier. The proposed scheme has not provided the facility for voice communication which is a prime need of combat operations. Moreover, to transmit and receive data to satellite, battery consumption power will be very high. Therefore, it is not feasible to be used for as a soldier’s hand-held device.

Cho et al. (2008) presented an infrastructure which relies on Unmanned Aerial Vehicles (UAVs) for transferring medical information of soldiers in battlefield to base camp (command and control center). Each soldier’s
symptoms are collected through sensors, aggregated and shared with other soldier nodes in the range via the blue tooth scheme. A UAV periodically arrives and hover at the battlefield. The soldier nodes transfer their data to UAV through IEEE802.11g. Multiple soldier nodes will be ready to transfer its data to UAV but one having more amount of data than others will be allowed. The flaw in this scheme is that it is not efficient to maintain database on each node because high computational resources would be required. Furthermore, it is not always necessary that data of each soldier would reach to UAV as all nodes may not always be in the Bluetooth range.

Gondalia et al. (2018) used machine learning to propose soldiers health monitoring system based on Internet of Things (IoT). It provides GPS coordinates for the injured and lost soldiers. A wireless body area network is used to identify such soldiers and K-Means Clustering technique is used to monitor the health status of soldiers that is, injured or death. Iyer and Patil (2018) targeted military applications and proposed an IoT based tracking and mobility sensor. The sensor was developed to ensure the safety of soldiers during war. The design consists of an Arduino board and multiple sensors to capture the vital signs of the remote human. The exact location of the soldier is tracked with the help of GPS that provides the longitude and latitude of the location. Moreover, the designed sensor also provides the body temperature of the human. It is a low cost and portable solution.

Stergiou, Psannis, Plageras, et al. (2018) studied latest technologies to support intelligent media transfer. In this study, various open source tools and simulators are examined. The tools are helpful in understanding the processing, storage, collection and management of big data. CloudSim is used as a simulator along with Cooja emulator to accomplish the study and test a single network segment. It can provide a start point for systematic data transmission in battle field. In another study, Stergiou, Psannis, Kim, et al. (2018) targeted the security aspects of IoT and cloud computing and presented a detailed survey. They highlighted the benefits of integration of these two technologies, presented their common features, analyzed security challenges and concluded that their combination can be helpful to improve the overall efficiency of the IoT based applications.

Psannis et al. (2018) presented an intelligent encoding technique for big data to support advanced scalable media applications on cloud computing systems. In order to evaluate the performance of the proposed technique, they compared it with High Efficiency Video Coding (HEVC) standard and claimed that their proposed technique is more efficient. This technique can also be integrated into HEVC. Ahuja and Banga (2019) conducted a case study to detect the mental stress of university students based on machine learning algorithms. This work collects data from 206 student’s is collected one week before the exam. Four algorithms are used for classification, including Support Vector Machine (SVM) Random Forest, Naı¨ve Bayes and Linear Regression.

To evaluate the performance of these algorithms, accuracy, specificity, and sensitivity are used as the performance evaluation parameters. The results show that SVM outperforms the others in terms of accuracy that is, 85.71%.

Vuppalapati et al. (2018) presented a machine learning model for the detection of mental stress. In this work, a mobile application (iOS device) has been developed that sends alerts to the user after computing the mental stress at four levels. The user’s Electroencephalogram (EEG) signals act as major parameter to compute the stress level. The performance of this system is highly correlated with the accuracy of the machine learning algorithm and its datasets. Cesur et al. (2013) discussed the post war psychological effects on soldiers which took part in combat operations. These soldiers suffer from post-traumatic stress disorder (PTSD) in comparison with those who were not part of such operations. Moreover, the detailed analysis revealed that the from direct firefight and having a tendency of suicides and PTSD.

Bray et al. (2001) studied the effect of stress on performance of army personals. They investigated that persons experiencing an average level work stress perform more efficiently as compared to those who suffer from low or high level of work stress. They also studied multiple psychological, physiological and social factors on the health of such persons. Masood & Alghamdi(2019) proposed a convolutional neural network (CNN) based framework to model mental stress. They monitored multiple physiological signals that is, breathing pattern irregularities, skin conductance, and heart rate variation through wireless sensors. They conducted several cognitive experiments to develop a set of protocols. In this work, cerebral features are extracted along with traditional physiological features from the neural signals. They concluded that neural signals helped in improving the efficiency of the developed model.

Venkatasubramanian et al. (2008) presented a novel key agreement protocol for sensors in Body Area Network (BAN). This protocol incorporates a soldier’s physiological symptoms such as photo plethysmogram (PPG) signals as a reference value for key generation at run time. The generated key is used to provide secure unicast communication between the nodes without any need of predefined key. Its main objective is to avoid the need of pre-configuration of the selected node at battlefield and provide plug and play mechanism for induction.
of any new node in BAN. The proposed scheme is not suitable for resource constraint devices because communication between nodes with one time pad key is a resource intensive task.

It can be reported that the available literature has focused mainly only on a few particular aspects. Some studies have emphasized only on key management without suggesting any cryptographic algorithm while others have proposed various secure communication mechanism without suggesting any communication technologies. Encryption of data is also a concern in some research papers. Moreover, a few researchers have also developed soldiers’ mental health assessment and monitoring system for battlefield scenarios. However, a comprehensive framework is required that should not only provides flexible and secure mechanism for battlefield communication but also helps in monitoring health status, tracking and avoiding the misuse of soldiers equipment. The framework should be efficient to be used by the devices with limited power.

The Proposed Framework

The proposed framework is divided into five stages. First stage is concerned with communication within the body of soldiers. Second stage is related to availability of communication among the soldiers, vehicles, and the command and control center. Third stage is related to manage the whole communication scenario whereas in the fourth stage, mental stress is computed. Fifth stage is related to preventing the misuse of soldiers’ equipment by the enemies in various situations such as hostile, injured, and death etc. The block diagram of the proposed framework is shown in Figure 1. It demonstrates the functionality of each layer for the proposed framework.

Stage 1: Intra Node Communication

The soldiers are equipped with various devices which aid them in the battlefield. The devices include GPS receiver, Head mounted camera, Voice communication system, Gyroscope, Accelerometer, Heart rate monitor, respiration sensor, Electrodermal Activity (EDA) sensor and Electromyography (EMG) sensor as shown in Figure 2. All of the devices and sensors constitute a single Wireless Body Area Network (WBAN) on the body of each soldier.

The communication among these devices and sensors is called intra node communication. All devices and sensors which are deployed in WBAN of the soldier are dedicated to a single Body Network Coordinator (BNC).

All these devices send data to BNC, which aggregates the received data. The GPS provides real-time location of the soldier. Head mounted camera is used to provide visual display to the communication vehicle and control center (Rizwan et al., 2020). Heart beat and respiration sensors provide information for monitoring the soldier’s aliveness. Gyroscope and Accelerometer (Chandrasekharan et al., 2016) provide orientation and posture information of a soldier. EDA sensor is used to find the changes in skin conductance due to nervous system activity. EMG sensor is used to record small electrical signals generated by human muscles movement.

These devices use ZigBee technology for sending its data to BNC. BNC aggregates the data received from the devices and forward to IEEE 802.11ah station carried by
each soldier. The station transfers the received data to the communication vehicle.

**Stage 2: Inter Nodes Communication**

To provide communication among the soldiers and from soldiers to communication control vehicles, different technologies can be employed such as ZigBee, Bluetooth, UWB and 802.11 a/b/g/n/ah WLAN etc (Aust et al., 2012; Baronti et al., 2007; Kabale, 2019; Kumar et al., 2015; Luinge & Veltink, 2005; Mpitziopoulos et al., 2009; Sun et al., 2013). However, in terms of providing infrastructure mode communication with long range and low power consumption, IEEE 802.11ah is more appropriate. The IEEE 802.11ah has a dominant feature of providing Non Line of Sight (NLOS) communication with ranges up to 1 km. IEEE 802.11ah Access Point (AP) is installed at communication vehicles which interconnects all stations (soldiers) in its infrastructure mode. So the distance between the soldiers and communication vehicle should not exceed 1 km. However, in case of distance beyond 1 km or low signal coverage, an intermediate 802.11ah relaying station is deployed to extend the range (Lipmaa et al., 2000). The relaying stations can also help to provide coverage in a scenario where distance between soldiers and communication vehicle is less than 1 km but there is a lack of coverage due to any obstacle between the communication vehicle and soldiers such as small hill or un-leveled battlefield as shown in Figure 3.

It is also recommended to use 802.11ah mounted drone to provide relaying facility for an additional aerial view of the battlefield. In case of destruction of communication vehicle or loss of communication between soldiers and communication vehicle, one of the soldier’s 802.11ah stations acts as an AP according to a defined priority as shown in Figure 3. In case of failure of current AP, next soldier’s station may act as an AP. So the information received by 802.11ah station of the soldier from BAN would be sent to the communication vehicle periodically and uninterrupted. If there are no significant deviations from previous averaged values of the readings of BAN sensors, only keep-alive message are sent periodically to the communication vehicle to conserve power. As soon as the significant deviation is received, the information is sent to the communication vehicle immediately.

**Stage 3: Security (Securing Communication)**

One of the basic aspects of military communication is security. Various encryption algorithms like 3DES, AES, IDEA etc. are used for securing the communication in traditional networks, but these encryption algorithms cannot be implemented in resource constraint devices (having limited battery and processing capabilities) on a soldier’s body. The proposed framework uses AES Counter mode (AES-CTR) in BNC for data encryption and decryption (Xinfeng & Wang, 2012).

Figure 4 shows the AES-CTR encryption and decryption process of the proposed framework. For data encryption with AES-CTR, the plaintext ($P_i$) is partitioned into 128-bit blocks. The final block can be less than 128 bits. $P = P_1, P_2, P_3, P_4, \ldots, P_N$. Each block $P_i$ is XORed with a intermediate cipher (block of the key.
stream) to generate the ciphertext \( C_i \), \( C = C_1, C_2, C_3, C_4, \ldots C_N \). The AES encryption of each counter value results in 128 bits of intermediate cipher (key stream). Initially, 32 most significant bits of counter are set as nonce value, followed by 64 bit per-packet IV value and the 32 least significant are set to one. This counter value is incremented by one to generate subsequent counter values, each resulting in another 128 bits of key stream.

The encryption of \( N \) plaintext blocks is summarized in Algorithm 1.

The AES() function is used to performs AES encryption with the updated key. The TRUNC() function truncates the output of the AES encryption to the same
Algorithm 1. AES-CTR Encryption.

1: $CTRVAL = \text{Nonce} \parallel IV \parallel \text{Zero}$
2: for $i = 1$ to $N-1$ do
3: $C[i] = P[i] \oplus AES(CTRVAL)$
4: $CTRVAL = CTRVAL + 1$
5: end for
6: $C[N] = P[N] \oplus TRUNC(AES(CTRVAL))$

Algorithm 2. AES-CTR Decryption.

1: $CTRVAL = \text{Nonce} \parallel IV \parallel \text{Zero}$
2: for $i = 1$ to $N-1$ do
3: $P[i] = C[i] \oplus AES(CTRVAL)$
4: $CTRVAL = CTRVAL + 1$
5: end for
6: $P[N] = C[N] \oplus TRUNC(AES(CTRVAL))$

length as the final plaintext block, returning the most significant bits. The decryption of N ciphertext blocks is summarized in Algorithm 2.

**Optimization of AES-CTR.** The prime benefit of AES-CTR is that intermediate cipher texts can be computed in advance and also be implemented in parallel. The intermediate cipher text (to be generated) depends upon counter values that can also be determined in advance. In this work, 512 intermediate cipher texts, each of size 128 bits, are calculated in advanced and stored in the buffer. For encryption and decryption of data, XOR operation of data block with an intermediate cipher text (access from buffer) is performed at run time. Figure 5 describes the optimized AES-CTR encryption and decryption process. XOR operation is one of the fast logical operations which can be efficiently implemented in hardware and has very low latency in contrast with other arithmetic operation such as multiplication. It also helps in power saving.

**BNCs configuration.** All soldiers BNCs are pre-configured with AES-CTR intermediate cipher text keys before deployment. Communication server generates a unique soldier ID (SID) and intermediate cipher texts for each soldiers’ BNC. It is noticeable that BNC has at least 8 KB permanent memory to store 512 intermediate cipher texts each of size 128 bits. BNC uses these intermediate cipher texts for encryption of data by XORing it with plain text data block as shown in Figure 5. BNC configuration process is shown in Figure 6.

**Protocol data unit (PDU) format.** Devices send the information of soldier (such as voice communication, heartbeat, respiration, and GPS location etc.) to its corresponding BNC which aggregates (Nguyen et al., 2015) the data and constructs the PDU. PDU contains various fields that contain key identifier, SID, payload, and time stamp as shown in Figure 7.

The SID (Soldier ID) field will enable the receiver to determine that it has successfully decrypted the PDU. The Payload field contains the data (received from devices and sensors). To prevent replay attack, Timestamp is attached to PDU. The key identifier (Jiang et al., 2017) enables the receiver to select proper key for decrypting the PDU.

**Data transmission.** The command and control center analyzes the received information and directs the soldier according to the combat strategy. The received information at communication vehicle is also being used to track soldiers in battlefield. At the receiving end, receiver extracts the key identifier from the received block and uses corresponding intermediate cipher text for decrypting the information (as carried out by sender for encrypting the block).

**Stage 4: Computation of Mental Stress**

Mental stress is caused by the external environment factors that is similar to fight or flight (run) situations on seeing a dangerous environment (an animal runs away when it feels someone can hurt him). The response to stressful situations produces hormones and muscles of legs and arms get ready to expand and respond to the situations. On normal conditions, the body is relaxed and organs work normally.

In the proposed system, a stress monitoring system is designed that would record real-time stress signals of soldiers during war times or operation against terrorists. The measured signals proportional to various stress levels, would provide a true representation of mental stress as stress inducing factors are real situations and challenges faced by soldiers during emergency times. The study would provide an objective assessment for mental stress and the ultimate goal is to represent stress by numbers as the practice is followed in blood pressure and sugar levels.

There are two phases for computing mental stress. In the first stage, three types of traditional physiological signals are recorded. Firstly, heart rate variations are monitored using heart rate monitors. Although ECG is gold standard for heart rate activity but it needs wiring and placement of electrodes which is not suitable in our proposed wearable system as it hinders daily routine activities. The heart rate monitoring from Polar Electro Inc. is proposed that is placed on a chest strap covering the heart of a soldier. For respiration changes, pulse...
oximetry sensor is used that is also attached to the chest strap. To record skin conductance, E243 electrodes are placed on the adjacent fingers of non-dominant hands so that hands of a soldier can move freely and there should be no obstacle for carrying and using arm weapons.

In the second stage, neural signals are monitored using the proposed wearable electrodes that are embedded in the cap of a soldier. In total, four ECL electrodes are mounted on the four corners of the cap. Cortical circuitry and cerebral signals are processed in the proposed EMG technique. A few artifacts such as eye blinking and muscle activities are pre-processed and filtered from the resultant neuro-biomedical signals to enhance the signal strength. The amplitude and frequency of neural signals provide variations in the levels of induced affects. A consciousness state of a person is determined by Alfa and Beta waveforms. The calm state and unconsciousness is denoted by Theta and Delta waves. In the state of stressful situations, Beta waves are more dominant and show more variations than Alpha waves whereas there are little changes in Alfa waveforms. Various features are extracted from Beta waveforms using Fourier transform.
and band pass filtering. Both lower body features and neural features are concatenated to form a feature vector that is employed in the classification stage to identify stressful situations in the warzone from the normal and routine activities. Although there are three classes namely, no stress, mild stress, and tense stress in our experiments but we have combined mild and tense stress into one class so that a situation whether it is low tense or high tense should be clearly distinguished from calm and peace situations.

**Stage 5: Misuse of Soldier’s Equipment**

The prevention of misuse of the soldier’s equipment by enemy is very critical. There may be various conditions such as hostile, injured, and death of the soldier in which enemy may access soldiers equipment that can be misused. To prevent the misuse, the framework handles various possible situations. The proposed framework has the capability to automatically detect the conditions (i.e., death, injured or hostile) and after detection, it acts accordingly. A series of experiments are conducted in the laboratory environment by simulating different scenarios of misuse. The obtained results are helpful in tweaking the functionality of this module to minimize the false alarms.

**Death.** To prevent misuse of soldier’s equipment in case of death, the heartbeat and respiration symptoms play a vital role. Soldiers’ heartbeats and respiration symptoms are continuously monitored by BNC. In a case where both symptoms disappear (soldier has died), BNC will automatically clear the stored configurations. BNC will also send an alert to all others nodes regarding the death of that particular soldier before clearing the configurations.

**Injured.** There may be a condition in which a soldier is unable to communicate due to injury or senselessness. To identify the condition of senselessness, GPS location information can be helpful. The location of the senseless soldier will not be changed over a period of time which will enable the communication vehicle to determine senselessness of the soldier.

But in combats, such situations are quite normal. Soldiers may not change their locations for longer periods of time. So to avoid any false alarms, communication vehicle first ask other nodes to report about that particular node. If something fishy is reported, communication vehicle sends clear command to BNC. If any enemy tries to snatch the communication equipment of senseless soldier, the heartbeat and respiration symptoms will not be available (these sensors are wirelessly connected to BNC with very low range) and upon absence of such symptoms the BNC will clear the stored configurations. There can be another critical situation where soldier is senseless and enemies are taking away him. This situation can be identified with the help of Gyroscope and accelerometer (Chandrasekharan et al., 2016). Both of these devices are used to provide orientation and posture information of the soldier. If the soldier is senseless (he is not communicating) and its GPS location is being changed, the orientation and posture information will enable the communication vehicle to determine that soldier is being carried away by enemies. In this situation the communication vehicle sends command to BNC for clearing the configuration.

**Hostile.** To prevent misuse of soldier’s equipment in case of hostile situation, there may be two options. Hostile soldier may clear stored configuration in BNC by pushing the erase button. Secondly, the communication vehicle (if it receives information from any other soldier about hostile condition of that soldier) can also send command to clear the BNC configuration of the particular soldier.

**Experimental Analysis**

This section presents the experimental evaluation of different modules of the proposed framework.

**Evaluation of Communication Modules**

The communication modules are evaluated in both Network Simulator-3 (NS-3) and outdoor environment. Several scenarios are created using NS-3 to test their efficacy. Multiple mobility scenarios of nodes are created and different performance metrics are recorded for example, delay, jitter, throughput, and reliability (packet delivery ratio). Table 1 reflects the overall environment setting for simulation. Tables 2 to 4 list the performance metrics with nodes mobility 2, 4, and 8 m/s, respectively.

The proposed system uses AES-CTR for encryption/decryption of data. The system’s throughput, delay, jitter and reliability are measured by varying nodes mobility. The results reflect that delay and jitter increase as the number of nodes are increased while packet delivery ratio and throughput only vary slightly by increasing the mobility increase or number of nodes. The simulation environment using NS-3 is presented in the Figure 8.

Furthermore, several experiments are also performed in the outdoor environment to test the efficacy of communication modules of the proposed system. Two persons are equipped with all the sensors, headphone, microphone, head-mounted camera, GPS module, BNC controller, 802.11ah station, etc. The configuration of BNC controller is performed as explained in the BNCs...
Configuration subsection. The persons are instructed to run fast, slow, stand still, and lay down for specified amount of time to collect and analyze the reading of the sensors. A car is used as communication vehicle that carried the AP of 802.11ah. The vehicle is moved in the radius of 1 km and received the data from two 802.11ah stations. After this, the vehicle is moved outside the radius of 1 km and another car equipped with 802.11 ah is used inside the given radius as a relay. Both of these communication scenarios are executed several times and successful communication is achieved.

Multiple interesting observations are recorded during the experiments and accordingly some tweaking is done to improve the proposed system. For example, one observation is that what would the system do if AP is destroyed? For such situations, one leader for the soldiers’ group formation is pre-assigned that would serve as an access point in case of communication vehicle’s destruction. It is quite logical because the leader is the sole in-charge now and would make sure to continue the combat activities. The system has the flexibility to add more nodes like it to increase reliability of the overall

| Parameters                  | Setting                        |
|-----------------------------|--------------------------------|
| Nodes                       | 5, 15, 25, and 50              |
| Mobility (m/s)              | 2.4, and 8                     |
| Mobility models             | Random way point               |
| Traffic                     | VBR                            |
| Routing                     | DSR                            |
| Transmit power              | 1.5 Mj                          |
| Receiving power             | 1.0 Mj                          |
| Channel type                | Wireless                        |
| Data size                   | 512 bytes                      |
| PHY standard                | IEEE 802.11ah                  |

**Table 1. Environment Setting Parameters.**

| No. of nodes | Delay (msec) | Jitter (msec) | Packet delivery ratio % | Throughput % |
|--------------|--------------|---------------|-------------------------|--------------|
| 05           | 1.05         | 1.04          | 97                      | 99           |
| 15           | 1.16         | 1.37          | 96                      | 97           |
| 25           | 1.76         | 1.73          | 98                      | 98           |
| 50           | 2.28         | 2.47          | 96                      | 98           |

**Table 2. Node Mobility = 2 (m/s).**

| No. of nodes | Delay (msec) | Jitter (msec) | Packet delivery ratio % | Throughput % |
|--------------|--------------|---------------|-------------------------|--------------|
| 05           | 1.25         | 1.41          | 98.6                    | 99           |
| 15           | 1.36         | 1.56          | 97.5                    | 97           |
| 25           | 1.91         | 1.90          | 98.3                    | 98           |
| 50           | 2.57         | 1.92          | 97.2                    | 98           |

**Table 3. Node Mobility = 4 (m/s).**

| No. of nodes | Delay (msec) | Jitter (msec) | Packet delivery ratio % | Throughput % |
|--------------|--------------|---------------|-------------------------|--------------|
| 05           | 1.75         | 1.11          | 98.2                    | 98           |
| 15           | 1.86         | 1.38          | 97.4                    | 97           |
| 25           | 1.91         | 1.62          | 99.3                    | 99           |
| 50           | 2.92         | 2.22          | 96.2                    | 96           |

**Table 4. Node Mobility = 8 (m/s).**
proposed system. Another observation recorded is to use the drone based 802.11ah station as a relay backup node. It would help in terrains having more obstacles. One more observation is that a particular sensor or sensors of some node stop working. So the particular information about a soldier is not recorded by the communication vehicle. Such cases may raise false alarms. The proposed system is tweaked to accommodate such cases. All soldiers of that formation would be informed about that node. The adjacent node would report about the status of that node whether it is fine, injured, or dead to avoid false alarms.

Another interesting issue raised during testing of the system is the optimal placement of BNC on the body of the soldier. Several positions like head, chest, legs, etc. are tested and communication results are obtained and compared. It is found that the BNC should be placed somewhere in between the chest and belly to get the maximum throughput and efficiency.

**Evaluation of Mental Stress Computation Module**

In experiments, the stressful situations are simulated to induce stress on the participants. In this work, 18 subjects are involved in the cognitive experiments that contain a range of activities. Firstly, various stroop tests are used to induce mental stress on the participants in indoor controlled conditions. The cognitive experiments contain memory tests for entering six digits on the screen in the reverse order, mirror test where images have to be redrawn by showing upside down pictures. In another test, various colors and texts are shown and the participant has to enter the correct choice using either text or color or sound. The purpose of all these activities is to observe stress related physiological parameters including heart rate variations, blood pressure changes, respiratory patterns, and body sweating. A wireless sensor based wearable platform is designed to capture heart rate variations, respiratory patterns, and sweating in index fingers. The biomedical signals are captured that are proportional to severity of the stress and wavelet transforms are used to perform filtering and processing to obtain digitization and sampling on the signals. For each sample, a number of physiological and neural signals were recorded and 12 features are extracted using statistical computations for mean, average, and power spectral densities of the raw signals.

In the feature extraction stage, Auto-regressive (AR) and Bird’s methods are used to extract useful parameters and information from the physiological signals. In AR method, a parametric approach is used to compute the power spectrum density (PSD) of the residual signals. In Bird’s method, PSD is estimated using the reflection coefficient in the forward and backward error prediction of the coefficients. In time frequency distribution (TFD) method, energy, power, frequency, and length of the principal track are used to compute the power features in the sampled signal. Sample entropy is also used to compute discriminant features.

The features are derived from the skin conductance signal and heart rate variability signal. The least square trending technique is used to compute the Skin Conductance Level (SCL) and Skin Conductance Response (SCR) for EDA signal. The mean (µ) and standard deviation (σ) of the residual signals SCL and SCR are computed using equations (1)–(4):

\[
\mu_{SCL} = \frac{1}{N} \sum_{i=1}^{N} SCL_i \quad (1)
\]

\[
\sigma_{SCL} = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (SCL_i - \mu_{SCL})^2} \quad (2)
\]

\[
\mu_{SCR} = \frac{1}{N} \sum_{i=1}^{N} SCR_i \quad (3)
\]

\[
\sigma_{SCR} = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (SCR_i - \mu_{SCR})^2} \quad (4)
\]

In the feature vector, a few measures from spectral signal of heart rate variability are also computed that contains low and high frequency ranges, successive RR intervals, RMS of successive differences of residual signals, and mean and average power of the signal. In the cognitive domain, brain signals in the form of Electroencephalography (EEG) waveform are analyzed.
and four statistical features are derived. In the left hemisphere of the brain, $\alpha_L$ and $\alpha_R$ represent left-side high filtered frequencies whereas in the right hemisphere $\beta_L$ and $\beta_R$ represent right-side high frequency spectrum. The ratios of the frequency spectrum, $\gamma_a$ and $\gamma_b$ denote the presence and severity of stress, respectively, that are defined in equation (5) and (6).

$$\gamma_a = \frac{\alpha_R - \alpha_L}{\alpha_R + \alpha_L}$$  \hspace{1cm} (5) \\
$$\gamma_b = \frac{\beta_R - \beta_L}{\beta_R + \beta_L}$$  \hspace{1cm} (6)

For classification, a Support Vector Regression (SVR) model is used to identify two classes, stressed (0 label) and relaxed intervals (1 label). The SVR model is trained for the indoor experiments and the same model can be used to identify stress in the real-time war situations. The model is trained on Python based Keras library. The system contains a graphic card of NVIDIA GeForce Titan processor. The Intel core i7 3770 processor with 3.2 GHz speed and 32 GB DDR3 was used for the training and test batches. In the training phase, 80% data samples are used whereas in the test set, 20% data samples are employed.

Table 5 presents the confusion matrix for the proposed technique. The algorithm correctly identified that there are 50 samples for True Positive (TP) who are in the relaxed class whereas 130 samples are identified to be in stressful activities (TN). There are 12 sample activities which are incorrectly detected as relaxed (FP) and 24 activities are wrongly stated as being stressful (FN).

Table 6 lists the performance evaluation metrics for the proposed model. It indicates that an accuracy of 83.33% is achieved.

### Quantitative Analysis and Discussion

It is observed that the following are the fundamental features that need to be provided by any good framework to fulfill the requirements of battlefield scenarios:

- Connectivity
- Security
- Flexibility
- Low Power
- Soldier Tracking
- Mental Health Assessment
- Handling Misuse of Equipment
- Physical Health Monitoring

In this work, a comparative analysis among proposed and existing techniques has been made on basis of above mentioned attributes. Table 7 enlists the features supported by the proposed and existing solutions. It illustrates that most of the existing solutions do not incorporate the essential features. Several studies highlight and discuss the importance of mental health assessment of soldiers during and after the war. None of these available techniques incorporates real time mental health assessment mechanism for soldiers in battlefield. The assessment of such important attribute is essential to carry out successful military operations and to reduce the death rate and suicidal tendency.

It is to be noted that the proposed framework not only incorporates secure communication along with flexibility and low power consumption but also addresses the physical and mental health monitoring along with soldier tracking and misuse of the equipment.

A score based mechanism has been designed for quantitative analysis. Let $S_i$ be the score assigned to each attribute. The value of $S_i$ is either 0 or 10. The score 10 is allocated to a provided attribute otherwise score 0 is assigned. This method is followed for the analysis of all attributes. Eq.7 is used for computing total score for all solutions based on the selected attributes.

$$\text{TotalScore} = \frac{1}{N} \sum_{i=1}^{N} 10 \times S_i$$  \hspace{1cm} (7)

Where, $N$ represents the number of features.

Table 8 depicts the normalized score of each solution. The solutions with higher score support more attributes. It illustrates that the proposed framework outperforms the techniques by 37.5% based on features-supported analysis. In short, the framework is comprehensive in its nature. It not only provides security with efficiency but also provides flexibility and reliability. Such a framework is the need of modern warfare and was a missing link in the existing literature of warfare.

Another aspect of the proposed framework is that it is quite flexible. It provides a blueprint for managing secure and reliable communication in the battlefield depending upon the war scenario and technology available. The
A layered approach of the framework helps to provide plug and play functionality inside the framework. Any layer of the framework can be replaced by the new layer according to the need by carrying a different technology. For example, the Bluetooth technology may replace the ZigBee technology (if required) as used in the stage 1 of the framework. In stage 2, IEEE 802.11ah may be replaced with any other WLAN standard depending upon requirements which make our framework more flexible. Moreover, any change in the underlying technology at both of these stages does not affect the working of other stages. The framework is efficient in terms of energy consumption. At different stages of the framework, multiple energy efficient techniques have been incorporated. At stage 1, ZigBee technology has been used for communication within WBAN because it is very efficient in term of battery power consumption. At stage 2, the communication between the soldier and the communication vehicle is reduced if there is no significant difference in sensor readings. Moreover, usage of IEEE 802.11ah also enabled the framework to be more energy efficient due to its small and efficient frame structure. Similarly, at stage 3, the proposed implementation of AES-CTR minimizes the computation on energy constraint devices while still retaining a high level of security. At stage 4, a mental stress health assessment is performed in a flexible way. The algorithm used at this stage can be modified or replaced at any time.

Misusing soldiers equipment by the enemy is a critical thing to prevent, and it has been briefly handled in the framework (stage 5). It is a sensitive issue as if not

Table 6. Experimental Results of Mental Stress Computation Module.

| Measure                        | Value | Derivation |
|--------------------------------|-------|------------|
| Sensitivity                    | 0.6757| \( \frac{TP}{TP+FN} \)  |
| Specificity                    | 0.9155| \( \frac{TN}{TP+TN} \)  |
| Precision                      | 0.8065| \( \frac{TP}{TP+FP} \)  |
| Negative predictive value      | 0.8442| \( \frac{TN}{TN+FP} \)  |
| False positive rate            | 0.0845| \( \frac{FP}{TP+FN} \)  |
| False discovery rate           | 0.1935| \( \frac{FP}{TP+FP} \)  |
| False negative rate            | 0.3243| \( \frac{FN}{TN+FN} \)  |
| Accuracy                       | 0.8333| \( \frac{TP+TN}{TP+TN+FP+FN} \)  |
| F1 score                       | 0.7353| \( \frac{2*TP}{2*TP+FP+FN} \)  |
| Mathews correlation coefficient| 0.6202| \( \sqrt{\frac{TP*TN}{(TP+FP)*(TP+FN)*(TN+FP)*(TN+FN)}} \)  |

Table 7. Features-Based Comparison of the Proposed Framework With Existing Solutions.

| Techniques                      | Connectivity | Security | Flexibility | Low power | Soldier tracking | Mental health assessment | Handling misuse of equipment | Physical health monitoring |
|---------------------------------|--------------|-----------|--------------|-----------|------------------|--------------------------|-----------------------------|---------------------------|
| Gondalia et al. (2018)          | ✓            | x         | ✓            | ✓         | ✓                | ✓                        | x                          | ✓                         |
| DeCleene et al. (2001)          | ✓            | ✓         | ✓            | ✓         | ✓                | ✓                        | x                          | x                         |
| Nemeroff et al. (2001)          | ✓            | x         | x            | x         | x                | x                        | x                          | x                         |
| Durresi et al. (2008)           | ✓            | ✓         | x            | x         | x                | x                        | ✓                          | x                         |
| Watthanawisuth et al. (2011)    | ✓            | ✓         | ✓            | ✓         | ✓                | x                        | x                          | x                         |
| Sze-Toh & Yow (2002)            | ✓            | x         | ✓            | ✓         | ✓                | x                        | x                          | x                         |
| Cho et al. (2008)               | ✓            | x         | ✓            | ✓         | ✓                | x                        | x                          | ✓                         |
| Iyer and Patil (2018)           | ✓            | x         | ✓            | ✓         | ✓                | ✓                        | x                          | x                         |
| Proposed Framework              | ✓            | ✓         | ✓            | ✓         | ✓                | ✓                        | ✓                          | ✓                         |

Table 8. Score-Based Comparison of the Proposed Framework With Existing Solutions.

| Techniques                      | Total score |
|---------------------------------|-------------|
| Gondalia et al. (2018)          | 62.5        |
| DeCleene et al. (2001)          | 37.5        |
| Nemeroff et al. (2001)          | 12.5        |
| Durresi et al. (2008)           | 37.5        |
| Watthanawisuth et al. (2011)    | 37.5        |
| Sze-Toh & Yow (2002)            | 50          |
| Cho et al. (2008)               | 37.5        |
| Iyer and Patil (2018)           | 62.5        |
| Proposed Framework              | 100         |
detected, the enemy may use it to disseminate the false information which may cause severe damage to the opponent failing the whole combat plan. Moreover, misuse of soldier’s communication equipment (Granjal et al., 2015) may reveal critical information about communication security mechanisms which may increase threats for future attacks.

The use of 802.11ah also adds some reliability factor in the proposed framework. As the range of 802.11 ah is relatively large (Aysal & Barner, 2008; Blatt & Hero, 2006), so it is possible to keep communication vehicle at some safer distance from battlefield thus minimizing its chances of being damaged. In the worst case, if communication vehicle is damaged, even then the communication between soldiers would still continue as one of the node (soldier) would become the AP, as discussed in the framework. The relaying nodes feature of the framework also adds reliability in the cases where distance between soldier and communication vehicle is exceeded to 802.11 ah range.

Conclusion

This paper proposes a reliable framework for secure communication and mental health assessment of soldiers in the battlefield. The proposed framework not only fulfills limitations of the resource constraint devices but also provides an effective command and control system that mitigates mental stress and minimizes emergency situations such as death or injury of a soldier. Moreover, it ensures availability and data confidentiality in a simple and effective manner. It also efficiently caters the conditions of misuse of soldier equipment by the enemy. With the incorporation of embedded wearable wireless system containing heart rate sensor, respiration sensor, skin conductance and EMG sensor, real time stress, and depression of soldiers can be determined. Thus suitable measures can be taken to plan better strategies and train a soldier with a few anti stress activities for better preparation of war scenarios. The experimental analysis shows that the proposed mental stress computation module achieved 83.33% accuracy. Moreover, a score-based comparison with the existing techniques indicates that the proposed framework outperformed its counterparts with 37.5% improvement in the features supported analysis.

In future, more training data and other real time scenario that induce stress such as fire scenes where firefigh- ters have to save life by sacrificing their own life, would be incorporated in the proposed framework. In the next phase of research, a few efficient and robust techniques can be developed to address the issues of insider threats in the warfare scenarios.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research work is supported by Data and Artificial Intelligence Scientific Chair at Umm Al-Qura University, Makkah City, Saudi Arabia.

ORCID iD

Muhammad Asif https://orcid.org/0000-0001-6811-0044

References

Abrami, S., Anbarasi, A., Hemalatha, T., Pavithra, A., & Mathiazhagan, V. (2017). Soldiers health and position monitoring system. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(2), 229–231.

Ahuja, R., & Banga, A. (2019). Mental stress detection in university students using machine learning algorithms. Procedia Computer Science, 152, 349–353.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422.

Ali, N. M., Sing, G., Yee, C., Kang, T., Chee, T., Ab Rashid, M., Sulaiman, M., Razi, A., Hasan, Z., & Abidin, A. (2018). A review of different applications of wireless sensor network (WSN) in monitoring rehabilitation. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(1-9), 121–127.

Aust, S., Prasad, R. V., & Niemeegeers, I. G. (2012). IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi [Conference session]. IEEE International Conference on Communications. pp. 6885–6889. New York: IEEE.

Aysal, T. C., & Barner, K. E. (2008). Sensor data cryptography in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 3(2), 273–289.

Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. Computer Communications, 30(7), 1655–1695.

Blatt, D., & Hero, A. O. (2006). Energy-based sensor network source localization via projection onto convex sets. IEEE Transactions on Signal Processing, 54(9), 3614–3619.

Bray, R. M., Camlin, C. S., Fairbank, J. A., Dunteman, G. H., & Wheeless, S. C. (2001). The effects of stress on job functioning of military men and women. Armed Forces & Society, 27(3), 397–417.

Cesur, R., Sabia, J. J., & Tekin, E. (2013). The psychological costs of war: Military combat and mental health. Journal of Health Economics, 32(1), 51–65.
Chandrasekharan, S., Gomez, K., Al-Hourani, A., Kandeepan, S., Rasheed, T., Goratti, L., Reynaud, L., Grace, D., Bucaille, I., Wirth, T., & Allsopp, S. (2016). Designing and implementing future aerial communication networks. *IEEE Communications Magazine, 54*(5), 26–34.

Chhabra, J. S., Chhajed, A., Pandita, S., & Wagh, S. (2017). GPS and IoT based soldier tracking & health indication system. *International Research Journal of Engineering and Technology (IRJET), 4*, 1228–1232.

Cho, D.-K., Chang, C.-W., Tsai, M.-H., & Gerla, M. (2008). Networked medical monitoring in the battlefield [Conference session]. *IEEE Military Communication Conference (MILCOM)*, pp. 1–7. New York: IEEE.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*(2), 544–546.

Cotton, S. L., Scanlon, W. G., & Madahar, B. K. (2009). Millimeter-wave soldier-to-soldier communications for covert battlefield operations. *IEEE Communications Magazine, 47*(10), 72–81.

DeCleene, B., Dondeit, L., Griffin, S., Hardjono, T., Kiwior, D., Kurose, J., Towsley, D., Vasudevan, S., & Zhang, C. (2001). Secure group communications for wireless networks [Conference session]. *IEEE Military Communications (MILCOM) Proceeding Communications for Network-Centric Operations Creating the Information Force. vol.I*, pp. 113–117. New York: IEEE.

Durresi, A., Durresi, M., & Barolli, L. (2008). *Secure mobile communications for battlefields* [Conference session]. IEEE International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), pp. 205–210. New York: IEEE.

Gondalia, A., Dixit, D., Parashar, S., Raghava, V., Sengupta, A., & Sarobin, V. R. (2018). IoT-based healthcare monitoring system for war soldiers using machine learning. *Procedia Computer Science, 133*, 1005–1013.

Govindaraj, A., & Banu, D. S. S. (2013). GPS based soldier tracking and health indication system with environmental analysis. *International Journal of Enhanced Research in Science Technology & Engineering*, 2(12), 46–52.

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312.

Hutzell, E. C. (2017). *Down the lines: US Army Communications in Europe, 1942-1945* [Master of Arts (History) thesis, Sam Houston State University, Huntsville, Texas], 1–73.

Iyer, B., & Patil, N. (2018). IoT enabled tracking and monitoring sensor for military applications. *International Journal of Systems Assurance Engineering and Management, 9*, 1294–1301.

Jee, H., Lee, K., & Lim, J. (2017). Autonomous maneuvering of relay UAV for battlefields using TDOA localization [Conference session]. *IEEE Military Communications Conference (MILCOM)*, pp. 453–458. New York: IEEE.

Jiang, Q., Zeadally, S., Ma, J., & He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access, 5*, 3376–3392.

Kabalci, Y. (2019). IEEE 802.15. 4 technologies for smart grids. In *Smart grids and their communication systems* (pp. 531–550). Springer.

Kumar, S., Lim, H., & Kim, H. (2015). Hierarchical MAC protocol with multi-channel allocation for enhancing IEEE 802.11 ah relay networks [Conference session]. *IEEE Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1458–1463. New York: IEEE.

Lipmaa, H., Rogaway, P., & Wagner, D. (2000). Comments to NIST concerning AES modes of operations: CTR-mode encryption. National Institute of Standards and Technologies. pp. 1–4.

Luinge, H. J., & Veltink, P. H. (2005). Measuring orientation of human body segments using miniature gyroscopes and accelerometers. *Journal of Medical and Biological Engineering and Computing, 43*(2), 273–282.

Masood, K., & Alghamdi, M. A. (2019). Modeling Mental Stress using a deep learning framework. *IEEE Access, 7*, 68446–68454.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials, 11*(4), 42–56.

Nemeroff, J., Garcia, L., Hampel, D., & DiPierro, S. (2001). Application of sensor network communications [Conference session]. *IEEE Military Communications Conference (MILCOM) Proceeding Communications for Network-Centric Operations: Creating the Information Force. vol.I, pp. 336–341. New York: IEEE.

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks, 32*, 17–31.

Nikam, S., Patil, S., Powar, P., & Bendre, V. (2013). GPS based soldier tracking and health indication system. *International Journal of Advanced research in Electrical Engineering, 2*(3), 1082–1088.

Psannis, K. E., Stergiou, C., & Gupta, B. B. (2018). Advanced media-based smart big data on intelligent cloud systems. *IEEE Transactions on Sustainable Computing, 4*(1), 77–87.

Radhappa, H., Pan, L., Xi Zheng, J., & Wen, S. (2018). Practical overview of security issues in wireless sensor network applications. *International Journal of Computer Applications, 40*(4), 202–213.

Rahman, R. U., & Tomar, D. S. (2018). Security attacks on wireless networks and their detection techniques. In K. Arya, R. Bhadoria, & N. Chaudhari (Eds.), *Emerging wireless communication and network technologies* (pp. 241–270). Springer.

Rizwan, M., Asif, M., Ahmad, M. B., & Masood, K. (2020). *PARK MY RIDE: Your true parking companion* [Conference session]. Springer 2nd International Conference on Intelligent Technologies and Applications (INTAP2019), pp. 695–710. Springer.

Saad, M., Bin Ahmad, M., Asif, M., Masood, K., & A. Al Ghamdi, M. (2021). Social distancing and isolation management using machine-to-machine technologies to prevent...
pandemics. *Computer, Materials & Continua*, 67(3), 3545–3562.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, 78(3), 964–975.

Stergiou, C., Psannis, K. E., Plageras, A. P., Ishibashi, Y., & Kim, B.-G. (2018). Algorithms for efficient digital media transmission over IoT and cloud networking. *Journal of Multimedia Information System*, 5(1), 1–10.

Sun, W., Choi, M., & Choi, S. (2013). IEEE 802.11ah: A long range 802.11 WLAN at sub 1 GHz. *Journal of ICT Standardization*, 1(1), 83–108.

Sze-Toh, K. S., & Yow, K. C. (2002). *Usage of mobile agent in configuring WPANs* [Conference session]. IEEE International Conference on Control, Automation, Robotics and Vision (ICARCV). vol.2, pp. 938–943. New York: IEEE.

Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. (2008). Plethysmogram-based secure inter-sensor communication in body area networks [Conference session]. IEEE Conference on Military Communications. pp. 1–7. New York: IEEE.

Vuppalapati, C., Khan, M. S., Raghu, N., Veluru, P., & Khursheed, S. (2018). *A system to detect mental stress using machine learning and mobile development* [Conference session]. International Conference on Machine Learning and Cybernetics (ICMLC). pp. 161–166. New York: IEEE.

Watthanawisuth, N., Tuantranont, A., & Kerdcharoen, T. (2011). *Design for the next generation of wireless sensor networks in battlefield based on ZigBee* [Conference session]. IEEE Defense Science Research Conference and Expo, pp. 1–4. New York: IEEE.

Xinfeng, B. A., & Wang, P. (2012). *Design of soldier status monitoring and command and control system based on Beidou system* [Conference session]. 2nd International Conference on Computer Science and Network Technology. pp. 1362–1366. New York: IEEE.