2016

Implementation of Secure 6LoWPAN Communications for Tactical Wireless Sensor Networks

Courtney, David W.

2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): 2016 IEEE Infocom MiseNet Workshop

http://hdl.handle.net/10945/50279

Implementation of Secure 6LoWPAN Communications for Tactical Wireless Sensor Networks

David W. Courtney and Preetha Thulasiraman
Naval Postgraduate School, Monterey, CA, USA
dwcourtn@nps.edu
pthulas1@nps.edu

Abstract— **Tactical wireless sensor networks (WSN) consist of power constrained devices spread throughout a region of interest to provide data extraction in real time. The main challenges to the deployment of tactical WSNs for mission-centric operations are limited nodal energy and information security. In this paper we develop security mechanisms to be implemented on a tactical WSN using the 6LoWPAN protocol for use by the United States Marine Corps (USMC). Specifically, we develop an architectural framework for tactical WSNs by studying security gaps and vulnerabilities within the 6LoWPAN security sublayer which is based on IEEE 802.15.4. We develop a key management scheme that is non-broadcast but that is also feasible in an operational scenario. In addition, we modify the 6LoWPAN packet structure to facilitate the newly developed keying mechanism. The tactical WSN architecture is designed to defend against a variety of network attacks that can potentially occur. Simulations will be conducted via MATLAB to show the effectiveness of the developed keying and communication mechanisms.**

I. Introduction

A wireless sensor network (WSN) is a group of sensor nodes geographically distributed to provide data gathering and monitoring of tasks and events. WSNs are finding increased applicability to the Department of Defense (DoD) in areas specific to tactical surveillance and reconnaissance. A WSN can be used to remotely monitor a battlespace, making the presence of a warfighter unnecessary thereby increasing the safety to forces and decreasing the cost of an operation. In addition, a WSN can be used to remotely monitor deployed systems and trigger alerts at a command and control site when certain events occur.

The WSN devices in use today by the United States Marine Corps (USMC) are known as AN/GSQ-257 Unattended Ground Sensor Set. The AN/GSQ-257 devices are part of the USMC's Tactical Remote Sensor System. The AN/GSQ-257s have multiple configurations that enable sensing of seismic/acoustic, magnetic, and/or infrared data [1]. This is helpful in performing perimeter enemy detection and tracking enemy movements offensively. The use of a WSN allows the USMC to remove the human element from possible danger while maintaining situational awareness with early detection from a remote location. Since WSNs are low powered devices, a different type of communication protocol that maintains a low energy cost wireless environment needs to be used. The IEEE 802.15.4 standard is a physical and data link communication protocol for low power personal area networks (LoWPAN) and is widely used in embedded applications for real time data extraction.

Since the IEEE 802.15.4 standard only defines the first two layers of the OSI model, another protocol must be used to provide full networking functionality for the WSN. The Internet Engineering Task Force's (IETF) 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) is a protocol designed to work with the IEEE 802.15.4 standard. 6LoWPAN is an open standard networking technology that standardizes Internet connectivity for low power wireless sensor networks. It alters the landscape by allowing IPv6 packets to be carried efficiently within link layer frames, such as those defined by IEEE 802.15.4, while reducing IP overhead.

A. Motives and Contributions

As the use of WSNs grow in the Marine Corps, it will become more attractive to potential attackers. In order to prevent a passive or active attack, multiple security methods must be implemented to maintain an efficient and effective WSN. Comprehensive defense security mechanisms must account for multiple types of attacks. Generally, to defend against an attack the military develops a defense model for the attack. Since there are multiple types of attacks, the military has developed multiple models to defend against each one. The development of a single model to defend against a variety of attacks prevents the need for an expanded arsenal of defense models saving the military money and manpower.

The USMC has high interest in WSNs and their ability to connect to a public domain. Currently, their WSN devices are deployed into the field, and their base station, known as AN/MSC-77, contains working spaces for two individuals to work inside of it [2]. The AN/MSC-77 is also known as the Combat Operations Center (CoC). The CoC includes a dedicated power source or a large generator to provide the power necessary to run all of the equipment within the AN/MSC-77. The CoC unit must also be in the vicinity of the WSN devices unless a repeater is used to place the unit in a more remote location. Currently, in order for the USMC to obtain the data from the WSN, an individual must physically go to the CoC, as it does not transmit the data acquired from

the WSN. Thus, the current data flow from legacy equipment and sensor devices lacks automation.

To facilitate seamless data delivery to and from the sensor devices, the network should be connected to another secure domain using a comprehensive communication protocol. The use of 6LoWPAN would significantly change the information flow as it currently exists by allowing multiple users in a unit to access sensor information despite their location. IP based information can be easily used to inform the situational awareness and common operational picture of the engaged unit.

6LoWPAN has been extensively studied in the literature but the focus has mostly been on single hop networks and energy consumption [3]. There have been studies that take into consideration an approach to implementing an efficient security mechanism for 6LoWPAN by either performing an analysis or survey [4, 5]. Only a limited amount of research has been conducted implementing a proposed security framework over a multi-hop 6LoWPAN network [6].

In this paper we propose a theoretical network design framework that uses 6LoWPAN and IEEE 802.15.4 such that it can be deployed for tactical operations by the Marine Corps. This theoretical framework is designed for a multi-hop static wireless sensor deployment scenario. Specifically, a command and control (administrative control) structure of the tactical WSN network is proposed. We incorporate and implement adjustments within the 6LoWPAN protocol packet structure that enables specific keying mechanisms and algorithms for confidentiality, authentication and integrity. Finally, the proposed steps in creating and deploying the secured tactical WSN will be examined.

It must be noted that this is a work in progress. The theoretical framework to solve the above mentioned issues will be discussed in this paper. In the coming months we will be testing this framework to determine the design feasibility. The desired end state for this research is to provide security solutions for 6LoWPAN that would pair with and enable current commercial sensor technology to be employed in austere and/or hostile environments to support Marine Corps Operations in a secure and energy efficient manner.

The remainder of this paper is organized as follows: In Section II we discuss the fundamentals of 6LoWPAN/IEEE 802.15.4. Section III provides a comprehensive discussion on the theoretical tactical WSN framework, including network design and setup, 6LoWPAN packet structure and security mechanisms and planned simulation setup. We conclude the paper in Section IV.

II. 6LoWPAN/IEEE 802.15.4 Fundamentals

There has been plenty of research to achieve security within a WSN [7]. There has been some work that has been done on tactical WSNs that serve as a foundation for our work [5, 6]. While [5] and [6] provide architectural constraints for tactical WSN deployment, the security mechanisms and its relationship with energy consumption is not discussed. In [8], the authors develop a cross layer load balancing/routing scheme for tactical WSNs. However, the routing mechanism does not provide for secure communications.

In order to develop a feasible secure design for tactical WSNs using 6LoWPAN, it is necessary to understand its packet structure. Considering the packet is reduced to a size of 127 bytes, some header information has been either removed or compressed. One of the fields within the header that was compressed was the addresses for the source and the destination. The address mode used reduces the IPv6 address from 128 bits (16 bytes) to 16 bits (2 bytes) which saves 14 bytes per address saving a total of 28 bytes [9].

Encryption within the 6LoWPAN environment is a requirement in order to have an effective tactical WSN and it has been addressed in the most recent release of the IEEE 802.15.4 standard [10]. Along with encryption there is an ability to add a method to ensure authentication called a Message Integrity Code (MIC). Knowing how encryption methods operate helps determine which one to use to defend against a variety of attacks. Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) is the suggested method within the 6LoWPAN standard. Within the encryption method, an Initialization Vector (IV) is used. The combined fields within the IV provide a unique value to be used along with the encryption key, creating a unique encrypted payload for each packet transmitted.

Another type of security mechanism is limiting the capabilities of the network. For instance, Network Discovery is a known vulnerability on 6LoWPAN networks [10]. Network Discovery is a method of finding neighboring nodes which the newly added node can route transmissions through. The vulnerability lies in verifying if the neighbor is a node that is authorized to access the WSN. A centralized, command and control tactical WSN architecture would mitigate some of these vulnerabilities.

III. Theoretical Framework

In this section we discuss the theoretical framework for the design and implementation of the tactical WSN using 6LoWPAN/IEEE 802.15.4. We discuss 1) the network design including the network devices used and their purpose; 2) the command and control parameters of the WSN which details specific tactical characteristics within the network (i.e., data routing and key management); and 3) the type of encryption used for the data is examined and determined.

A. Network Design

The proposed network design includes multiple elements, each serving a specific purpose. The elements included within the network architecture are as follows: master station (MS), base station/border router (BS), and sensor nodes. The proposed network architecture is shown in Fig. 1.

Master Station (MS): The MS serves as the central node of the network, as depicted in Fig. 1. The proposed MS is a modified AN/MSC-77 (CoC) currently used by the USMC. The modifications increase the capabilities of the CoC by

moving its location from the harsh environments where the WSN is deployed to a structured, fortified military base making it easier to protect and the data easily accessible. The proposed MS provides a universal connection to external domains, and accessibility and administrative privileges to the sensor nodes while located at a safe remote location away from the WSN. The MS has the ability to connect to each node within the internal domain since the WSN is able to communicate with each of the other individual elements. The MS also provides the user with a secure position to manage and control the WSN while obtaining the data from the WSN without having to rely on physically retrieving the stored data. Security for the MS has already been developed and tested throughout the military as it will not be operating within the network using 6LoWPAN. The MS will also be able to decipher the encrypted payloads sent to it from a 6LoWPAN device.

Base Station/Border Router (BS/BR): The BS is the transitional element within the WSN that connects the 6LoWPAN/internal environment to the public/external environment. This is also commonly known as a sink node. The proposed BS is essentially a secured router and transmits the data received from the WSN into an external domain to the MS. The BS receives packets from the nodes and removes unnecessary 6LoWPAN header information. It reassembles the payload into the external network packet structure in order to reach and be read by the MS. The BS also performs the same task in the reverse direction, removing unnecessary packet headers and adding the appropriate 6LoWPAN header to send the packet to the sensor nodes. Within the 6LoWPAN environment, the BS converts the addresses between the internal and external network environments since 6LoWPAN uses a modified addressing mode. The BS does not interfere with the payload because it is encrypted. The BS only contains the necessary encryption in order to connect to the MS, therefore the packet payload to be transmitted remains secure.

The BS will be restricted to 63 hops from the furthest node since the hop limit field within the packet structure will only consist of 6 bits (this will be further discussed in Section III-D). Since the BS connects the WSN to an external network, it will require either a dedicated electrical supply, a generator, or robust battery supply as more power is needed to transmit a signal strong enough to reach the external domain. Generally, each BS can be easily obtained at a lower cost than the total investment required to operate the AN/MSC-77 (CoC) in place near the WSN. The BS is also able to withstand the harsh environments in which it is deployed and is much smaller than the CoC since it does not need to have workstations available. The BS will also be tamper proof to prevent any physical modifications to the device as it is already implemented on the sensor devices in use [1]. Since the BS is smaller, it can also be concealed easier.

Sensor Node: The sensor nodes are the end elements. Each node is designed to attach to multiple types of sensors and to relay packets to the MS for compilation and analysis. The nodes are tamper proof and are assumed to have the sensor capabilities as described in the USMC manual [1], including which sensors can be connected, and which modes of operation

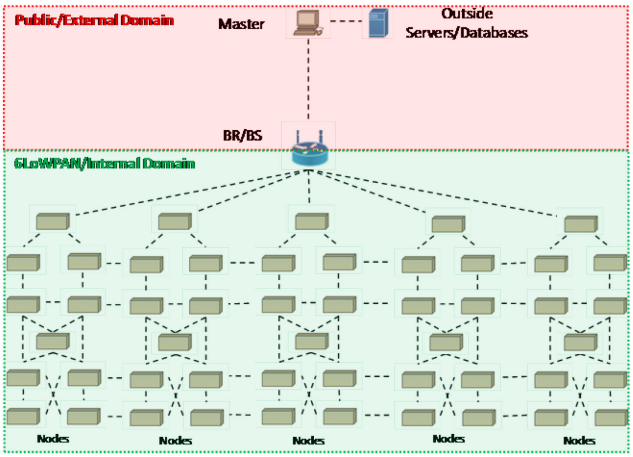

Fig. 1. Proposed 6LoWPAN network design

are offered. The sensor nodes communicate with the MS only through encrypted payloads.

Attack Mitigation for Network Design: Vulnerabilities associated with the design of this tactical WSN include single points of failure and physical protection of the sensor nodes. The MS and BS are single points of failure to the WSN and if removed, the network is no longer accessible and unable to be used. A denial of service (DoS) attack would exploit this type of vulnerability. The MS has a greater impact on the WSN since it provides reachability, accessibility, and administrative privileges to the sensor nodes. The BS can be replaced by another BS without affecting the encryption or payload data transmission between the nodes and MS. The vulnerability of the MS and BS is not the focus of this paper but the military does have similar devices in place today. Lastly, the physical protection of the nodes and BS remains an accepted risk.

B. *Command and Control (Administrative Control)*

The administrative control aspects of the WSN are critically related to its functionality as well as the implementation of its security mechanisms. In this paper, the security mechanisms implemented are controlled by the MS. The control mechanisms of the MS include node control, defined routing, and keying mechanisms. Using a centralized entity, such as the MS, to perform these functions, limits attacks on the network.

Node Control: The nodes will be controlled by the MS via encrypted payload. The encrypted payload will contain information which includes when the node will provide real time coverage or when the node will store detected events and transmit them in bulk at a later time [1]. This also removes the need to send an individual to the base station to make a modification or to place a new sensor required for a new task; instead the node can be adjusted immediately from the MS.

Defined Routing: The MS will maintain a directory of all of the networks connected to the BS as well as the nodes within each network. The MS will also be able to control each node's routing table. Each node will only be able to route to two nodes upstream (i.e., to the MS), with an exception for the nodes directly connected to the BS or when a node is deployed to a

location in which only one other node is within its wireless range. The node also performs in the same manner downstream, but the limitation of two nodes is not enforced in order to compensate for network expansion. This gives the MS the ability to implement energy cost saving measures within the network. Controlling the packet flow within the network is also a way to protect the network from outside attacks by not receiving and routing packets from invalid sources.

The defined routing allows the MS to add new nodes by adding the new node's address information into the neighboring node's routing table via the encrypted payload and adding the necessary routing table information to the new node during the setup. This method prevents the need for a neighbor discovery protocol which is noted as a vulnerability within 6LoWPAN in multiple sources [10, 11]. The MS can also remove compromised or expired nodes by removing the node from the neighboring nodes' routing tables, thus any data sent from the node will not be routed.

Fig. 2 is an example of the defined routing scheme of deployed sensors at an intersection. An intersection was used as an example since these devices track not only personnel but tanks or other manned vehicles [1]. The sensors are not limited to deployment at an intersection as they may also be deployed along a perimeter of a base or along a path of intended traffic. If an anomaly within the traffic flow occurs it may mean an impending attack or an attack by the enemy is already underway within the area. To provide full coverage of an intersection, sensors are placed on each side of the road. The primary and secondary routing paths are marked with every node having a secondary path except for the nodes with a direct link to the BS.

Fig. 3 demonstrates how the WSN is able to remove a node that has been compromised. The defined routing scheme is adjusted to not allow a packet to be transmitted to or from the compromised node since it is no longer in the routing tables within the WSN. The adjustments in the routing path did force some nodes to assume more of a load, but the WSN is able to remain effective until the compromised node is repaired.

Keying Mechanisms: A keying mechanism is needed in order to protect the information being transported between the nodes. Previous research from [10] determined that private keying is the most energy efficient method to transport the payload. With the use of a private key, each node will have a unique key which is only shared with the MS. As mentioned previously, the BS will not have any of the encryption keys shared between the nodes and the MS, but the BS will have a separate keying mechanism shared with the MS. The external network and the keying mechanism for the external network are already in use in other areas within the military and is not the focus of this paper.

Attack Mitigation for Administrative Control: Command and control allows for mitigating factors if the WSN has nodes that are attacked via man-in-the-middle (MITM) or DoS. Each of these attacks requires an individual or remote device to be near the WSN, but the attacker will be detected prior to performing the attack due to the sensor capabilities as previously mentioned above [1]. The defined routing prevents

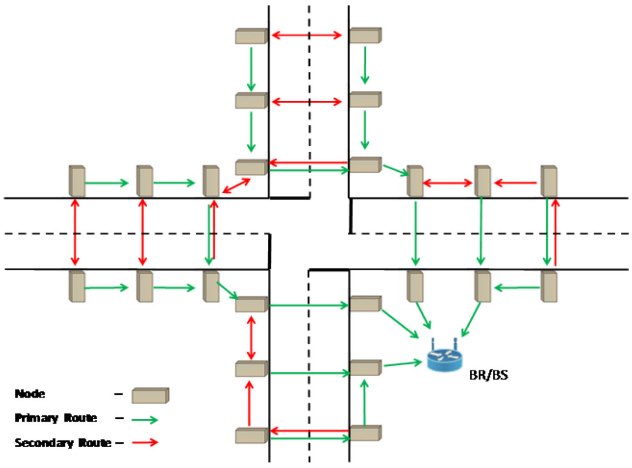

Fig. 2. Defined Routing Scheme

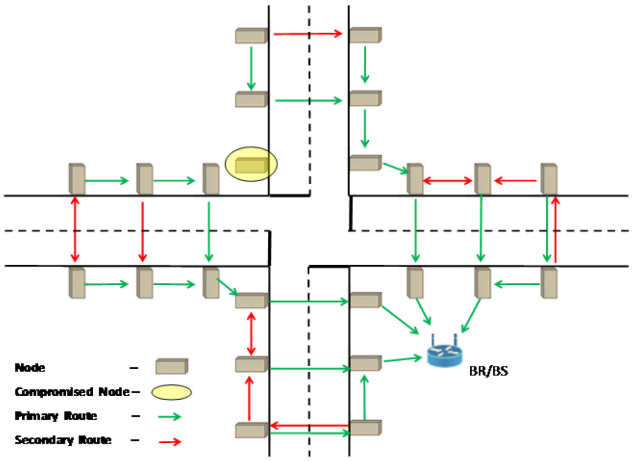

Fig. 3. Defined Routing Scheme (with compromised node)

the intruder from further infecting and draining the rest of the network's power resources. Use of a keying mechanism also protects the data during transportation over the network. Therefore the MITM or spoofing attacks will not be able to change any of the data nor will they be able to eavesdrop.

C. *Encryption*

Multiple types of encryption are available to us as keying mechanisms including the Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Rivest-Shamir-Adleman (RSA). Each encryption method is authorized by the National Security Agency (NSA) which sets the encryption standards for the Department of Defense and establishes key lengths set for the highest classification levels [12]. According to [10], the most recent IEEE 802.15.4 standard lists eight security modes ranging from no encryption (one mode) to different versions of AES (seven modes). As a result, AES is used as the keying mechanism in this paper. The seven modes of AES boast different levels of encryption and authentication. Since the devices being used can be located within a hostile environment and are interacting with government networks, the highest levels of security are

required within the WSN; therefore, the data must be encrypted and authenticated. To meet these requirements AES-CCM* with 128 bit keys is used as the keying mechanism to provide confidentiality, integrity, and authentication. The selected encryption also protects against MITM, spoofing, and eavesdropping attacks. The keying mechanism will be further discussed in the 6LoWPAN packet structure.

D. 6LoWPAN Packet Structure

The proposed 6LoWPAN packet structure is shown in Fig. 4 and is based on the packet structure defined in [13] with header compression schemes. However, the packet structure has been modified to incorporate the proposed security mechanisms. The fields within the packet structure are defined as follows:

Frame Control (2 Bytes): This field has been defined by the 802.15.4 standard with no changes made [14].

LOWPAN IPHC/LOWPAN NHC (2 Bytes Each): These fields have been defined by RFC 6282 [15] with no changes made.

Path (2 Bits) /Hop Limit (6 Bits): The proposed routing mechanism defined in this paper limits the direction each packet can take to reach the BS from the node. This mechanism is a modification from the proposed packet structure in [13]. Within the "Path/Hop Limit" byte, the first two bits are used to help the MS determine if there is an issue with a node routing packets while the final six bits limit the amount of hops a packet can take to 2^6-1 or 63 hops. Limiting the number of hops to 63 will not present an issue since the node next to the BS would not be able to support a large network of nodes to remain energy efficient. The first two bits will be used individually to determine whether the packet was transmitted over a primary or secondary route. The second bit is used only by the source node. In the event the primary route is used to send the packet, the bit is 0. If the secondary route is used then the bit is 1. The same method is applied to the first bit and is used by all nodes except the originating node. When the MS receives the packet, it is known if a node was not able to transmit to a designated primary node. Depending on the modes of operation selected, the MS may be able to determine which node may be off line or compromised instead of waiting for a response or detection. Specific attacks such as wormhole, sinkhole, black hole, and sybill attacks can be detected or even prevented by the designated routing and path bits.

Source/Destination Address (2 Bytes Each): The addresses are in the compressed 16 bit mode for a smaller overhead described within [15].

Initialization Vector (16 Bytes): The IV is used to help protect against replay attacks and is also used in the CCM* process to encrypt the payload [10]. The shaded area within Fig 4 is the proposed composition of the IV.

Source Port/Destination Port/CRC (2 Bytes Each) and Length of IP Header (1 Byte): These four fields have no changes or compression modifications [15].

Payload (71 Bytes): The payload is the amount of data that can actually be transmitted from the WSN. The data is encrypted, providing confidentiality during data transmission using the combination of the IV and the AES-CCM* 128 bit key.

Bytes 1	2	3	4
Frame Control		Source MAC Address (8 Bytes)	
Dest MAC (8 Bytes)		LOWPAN IPHC (2 Bytes)	Path/Hop Limit
Source IP Address		Desitnation IP Address	
LOWPAN NHC		Flags	Sequence Number
Sequence Number (4 Bytes)			Source Port
Source Port	Destination Port		Length of IP Header
Payload (71 Bytes)			
MIC (16 Bytes)			
Next Header	CRC		

Fig. 4. Proposed 6LoWPAN Packet Structure

Message Integrity Code (16 Bytes): To provide authentication and integrity, a MIC is created within the AES-CCM* mode of encryption and is attached to the end of the packet. The MIC is a hash unique to the packet and is used to verify that no changes were made to the original message. The MIC provides another layer of protection against any attack that tries to inject or change data being transmitted.

Next Header (1 Byte): It is used in higher layers and remains unchanged [15].

E. Transition

The transition of the packet from one domain to the other is to be completed by the BS as previously mentioned above. Since the 6LoWPAN packet contains necessary information for the MS to properly assess the effectiveness and efficiency of the WSN, the BS must transfer the necessary fields to the packet used on the external domain. Fields needed by the MS include the Path, IV, Payload, Next Header, and MIC. The designated Path bits are only required to make the transition when the message is coming from the node to the MS as the node cannot perform control commands and is not equipped to handle the analysis of paths taken by multiple nodes.

F. Deployment of Nodes

The deployment of the WSN will be similar to Fig.1. Creating the network first requires setup of the key exchange for encryption purposes, the routing table to be loaded, and evaluation of ideal physical placements for the nodes.

Key Exchange/Routing Table: After the network is designed and all of the routing tables have been constructed, the information for each node needs to be transferred to the node and BS. Each node and BS is physically connected to the MS for bootstrapping. The private key for the device and the constructed routing table is transferred to the node and BS. The routing table is transferred to the nodes by the MS to enable the nodes to connect to the network. The key exchange consists of a private key which is only shared between the MS and the node. The physical transfer of the key exists to prevent an enemy from gaining access to an entire network's information (MITM attack) simply by obtaining the key from one node. By using a private key unique to each node the enemy would only have access to that node's information. It will also allow the MS to remove the node from the network by adjusting routing

tables of surrounding nodes without compromising the rest of the network.

Physical Placement: While connected, the MS is able to maintain a geographical map of deployed nodes and map the deployment of any new node. This will help determine if the pending placement of the new node will be able to connect to surrounding nodes. This is critical to the deployment of the WSN since it will help track enemy movements and position.

Network Connection: Since the physical location of the node will be known and the surrounding nodes will be within reach, the placement within the network will also be determined. The MS can then add the node to the desired network. If the node is able to be added to multiple networks, then the MS is able to determine which network would be the most energy efficient network to add the node.

G. Simulation

We intend to test and evaluate the proposed theoretical framework in the coming months. The proposed WSN with the modified 6LoWPAN packet structure will be implemented and tested against a variety of attacks within a MATLAB simulated environment. The attacks that will be used are: MITM, spoofing, and a node focused DoS attack. The MITM attack will be focused on eavesdropping and changing the data as the packet is transmitted. This will help determine if the MS can detect whether the data was changed. Spoofing will focus on authentication and the simulation will confirm that the MS will notice the data received is not valid which will result in the removal of the node from the WSN. A node focused DoS attack will cause a node to fail and the simulation will confirm that the MS can detect the loss of the node, again leading to the node's removal from the WSN.

The attacks will be focused strictly on a network environment and will not provide any indications or warnings prior to being implemented. The purpose of the simulations is to determine if the attacks are defended against and detected, allowing for mitigations to take place, not to actually perform the mitigations.

IV. Conclusion

In this paper, we study the implementation of the 6LoWPAN protocol for tactical WSNs. We examine the need for 6LoWPAN in tactical WSNs used by the Marine Corps in operational scenarios. The 6LoWPAN protocol with the addition of necessary security mechanisms can be implemented and used by the USMC to boost the abilities of their current WSNs. In this paper, we develop and discuss a comprehensive tactical WSN framework using 6LoWPAN that includes a hierarchical network design using defined network devices. The use of a structured/centralized network design allows for secure network reachability and accessibility. We implement multiple security mechanisms within the 6LoWPAN protocol. These security features include encryption, authentication and integrity and are applied/implemented into the 6LoWPAN packet structure. We intend to evaluate our framework using MATLAB and test it against a variety of attacks in the coming months.

ACKNOWLEDGEMENT

This work has been funded and sponsored by the Marine Corps Systems Command (MCSC) in Quantico, VA, Grant Number NPS-N16-M296-B.

References

[1] *Unattended Ground Sesnor Set AN/GSQ-257 Technical Manual*, TM 09632A-OI, U.S. Marine Corps, Washington, DC, 2008.

[2] *Sensor Mobile Monitor System AN/MSC-77 Technical Manual*, TM 09856A-10/1A, U.S. Marine Corps, Washington, DC, 2008.

[3] A. Efendi, S. Oh, A. Negara, and D. Choi, "Battery-Less 6LoWPAN-Based Wireless Home Automation by Use of Energy Harvesting," in *International Journal of Distributed Sensor Networks*, vol 2013, 2013.

[4] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPANs) Routing, Request For Comments (RFC): 6606, May 2012.

[5] H. Song, S. Lee, S. Lee, and H. Lee, "6lowpan-based tactical wireless sensor network architecture for remote large-scale random deployment scenarios," in *Proc. of IEEE Military Communications Conference (Mil-Com)*, 2009, pp. 1-7

[6] S. Lee, S. Lee, H. Song, and H. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," *in Proc. of IEEE Military Communications Conference (MilCom)*, 2009, pp. 911-917.

[7] A. Callanan and P. Thulasiraman, "Achieving sink node anonymity under energy constraints in tactical wireless sensor networks," in *Proc. of IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 2015, pp. 186-192.

[8] K. White and P. Thulasiraman, "Energy effcient cross layer load balancing in tactical multigateway wireless sensor networks," in *Proc. Of IEEE International Inter-Disciplinary Conference on Cognitive Method in Situation Awareness and Decision Support (CogSIMA)*, 2015, pp. 193-199.

[9] S. Raza, S. Duquennoy, T. Chung, D. Yazar, and U. Roedig, "Securing Communication in 6LoWPAN with Compressed IPsec," in *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, pp 1-8.

[10] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communication Surveys & Tutorials*, vol. 17, pp. 1294-1312, Third Quarter, 2015.

[11] A. Rghioui, M. Bouhorma, and A. Benslimane, "Analytical study of security aspects in 6LoWPAN networks," in *5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 2013, pp. 1-5.

[12] National Security Agency (2015, Aug.*)*. NSA Suite B Cryptography. Suite B [Online]. Available: https://www.nsa.gov/ia/programs/suiteb_cryptography/.

[13] S. Raza, S. Duquennoy, and G. Selander, "Compression of IPsec AH and ESP Headers for Constrained Environments (Draft)," pp. 1-10, 2013, Sept. 2013.

[14] O. Hersent, D. Boswarthick and O. Elloumi, *The Internet of Things: Key Applications and Protocols.* Chichester, UK: John Wiley & Sons, Ltd, 2012.

[15] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, Request For Comments (RFC): 6282, Sept. 2011.