An Efficient Secure Algorithms to Mitigate DoS, Replay and Jamming Attacks in Wireless Sensor Network

C. K. Marigowda, Thriveni J, Gowrishankar S, Venugopal K. R

Abstract — Wireless Sensor Networks are by nature resource constrained, due to this characteristic, they are more vulnerable to different kinds of attacks. Protecting unauthorized users from accessing information stored in WSN is an important issue to be addressed. The proposed Synchronized Incremental Counter (SIC) mechanism focuses on security in WSN against Jamming and Replay attacks. Modified Constrained Function based Authentication (MCFA) algorithm is an AES with OCB mode, a symmetric key cryptography is used against Denial of Service (DoS) attack. The proposed collective methods effectively provide security without degrading the network performance with less packet loss and communication time, thus increasing the network lifetime.

Index Terms — Wireless Sensor Networks, Denial of Service, Replay, Jamming attack.

I. INTRODUCTION

Wireless Sensor Network (WSN) comprises of large number of autonomous, low cost, low power, wireless nodes and is utilized as part of different applications, for example, sensing and tracking in military, monitor environmental condition, and battlefield surveillance. At the point when WSN is deployed in un-observed, open, unreceptive environment, sensor nodes lead to high risk of being captured by an active attacker [1].

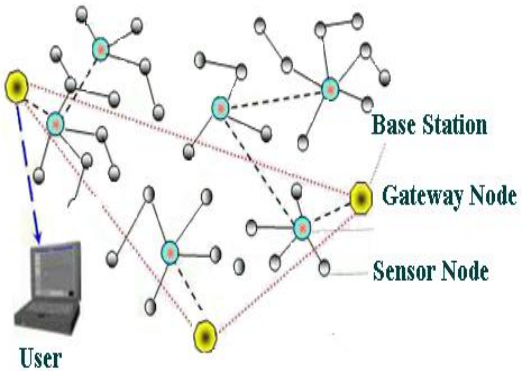

Fig. 1. Wireless sensor nodes deployment scenario

Manuscript received August 1st, 2018; revised August 10th, 2018

C. K. Marigowda is with Department of Information Science and Engineering, Acharya Institute of Technology, Visvesvaraya Technological University, Bengaluru, India (e-mail:marigowda@acharya.ac.in)

Thriveni J is with Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India (e-mail: drthrivenij@gmail.com)

Gowrishankar S is with Department of Computer Science and Engineering, B M S College of Engineering, Bengaluru, Karnataka, India (e-mail:gowrishankar.cse@bmsce.ac.in)

Venugopal K R is with Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India (e-mail: venugopalkr@gmail.com)

In addition to the inherent limitations in computing and communication, the deployed sensor nodes make them more vulnerable to various attacks in the network [2].

Three major attacks on WSN are discussed in this paper namely Jamming, Replay and DoS. In case of DoS attack, the attackers attempt to prevent legitimate users from accessing the service, usually attackers send excessive communication requests. Due to this the targeted system cannot respond to the legitimate users.

Jamming attack is a type of Denial-of-service attack against wireless medium with more severity. The target being packets of high significance and affects by emitting radio frequency signals. This results in congested routes with garbage packets and denies the legitimate systems from sending/receiving packets. Also it may delay or drop the delivery of legitimate packets.

Replay attack, is primarily man-in-the-middle attack. The adversary copies the message sent by source and sends it to the destination for more than once. If the targeted system cannot differentiate between the original message and its duplicate copies, then it results in malfunctioning. The adversary may replay messages as if they are authenticated, also can alter routing information resulting into routing loop or may exhaust resources of sensor nodes by repetitive messaging.

A. Motivation

The very fact that largely deployed sensor nodes depicted in Fig. 1 covering a vast area is easily exposed to attackers who may confine and reprogram such individual nodes. The opponent may use his own strategy of attacking and persuade the network to acknowledge them as legitimate nodes. Falsification of original data, hacking of collected network readings, extracting private sensed data and denial of service are certainly probable threats to the sensor networks and this compromises the security and privacy of WSN. These security issues are addressed by enhancing the software and hardware features. Development of new security mechanisms and security policies are challenging research issues in WSN.

B. Contribution

A Security mechanism on network layer of WSN is implemented. To provide security against DoS attack a mechanism called Modified Constrained Function based Authentication (MCFA) [3] with AES and OCB mode is proposed. Virtual Counter Manager (VCM) with Synchronized Incremental Counters is used to resist the replay and jamming attacks. The proposed algorithm provides high security and it operates with low energy.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Organization

The paper is structured as follows. Section II provides related work. The proposed method is illustrated in Section III. The results along with implementation features are discussed in Section IV and Final section concludes the work.

II. Related Work

Protocols such as SPINS [4], TinySec [5], ZigBee [6], and MiniSec [7] are considered as major technologies to provide security in WSNs. The protocol SPIN attains limited storage capacity by reusing crypto primitive code. However, drawback of SPIN is with respect to synchronization in a WSN [4]. TinySec is a major secure link layer protocol, it achieves low energy consumption and less memory usage. Limitation of TinySec is for efficient energy consumption the security features is diluted and it is fails in securing network from replay and resource consumption attack [5].

ZigBee is not limited with network wide key but it contains a per message counter as the Initialization Vector (IV) to secure network from replay attacks, ZigBee scores well against TinySec protocol for its strong security features. However, ZigBee is an expensive protocol as it sends 8-byte for each packet, resulting in high energy consumption and high communication overhead [8].

MiniSec is a secure protocol for network layer. It consumes less energy compared to TinySec and is on par with ZigBee in security aspects. Drawback in MiniSec protocol is that, it consumes more energy whenever packet loss occurs [9]. Other existing methods, LLSP and LEDS ensure authentication, access control, confidentiality for the message and protection against replay attack. But they have low performance overhead. R-LEAP+ protocol has its own approach for security from replay and jamming attacks, but in practice it is computationally intensive for resource-limited Wireless Sensor Networks.

Chia-Mu Yu et al., [10] have proposed a scheme called Constrained Function-based message Authentication (CFA), which is based on hash function and it supports the functionality of en-route filtering. The proposed mechanism addresses the DoS attack but this technique does not provide security against Jamming and Replay attacks

Marco Tiloca et al., [11] have proposed the effect of selective jamming attack in Time division multiple access (TDMA) WSN ie., typically slots are pre-allocated to sensor, and every slot is used by the same sensor node for a number of successive super frames. an opponent could prevent a victim sensor node communication by just jamming its slots. Proposed JAMMY is a distributed and dynamic mechanism for providing security against selective jamming in TDMA-based WSNs the proposed technique not addressed DoS and Replay attacks.

In nutshell a comparison of some well-known security methods are depicted in Table I. Though these methods are popular in providing a higher level of security in WSN they fail to deliver optimally for security against the three aforementioned critical attacks

TABLE I
COMPARISON OF A FEW STATE-OF-THE-ART METHODS

Security Mechanism	Replay attack	Jamming attack	DoS attack
SPIN	Yes	Yes	No
MiniSec	Yes	Yes	No
TinySec	No	No	No
ZigBee	Yes	No	No
Proposed	Yes	Yes	Yes

III. SYSTEM MODEL

This section brings out the topology of WSN used in the proposed method and the attack models.

A. Network Topology

The structure of the Network is shown in Fig. 2. The Sensor Network is divided into zones [12]. Each zone comprises of three types of nodes viz. Base Station (BS), Cluster Head (CH), and Functional Sensor Node (FN). Sensor nodes monitor the physical condition and transfer the sensed information to the base station. Due to the less communication range of sensor nodes a cluster head is incorporated in each zone for aggregating the data from FNs and communicate to base station. The base station holds abundant resource that can query data by request of wireless link connected to all CHs [8].

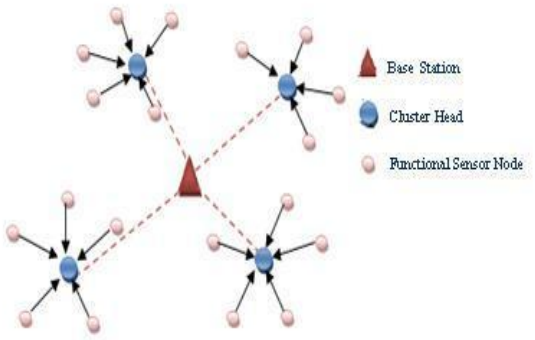

Fig. 2. Network topology

B. Attack Model

WSN, communications are broadcast in nature, therefore attackers can easily intercept, eavesdrop, inject and alter transmitted data and it is difficult to provide security. In WSN attackers are not only restricted to use hardware of sensor network; they also access the network remotely with the help of highly powerful radio transceivers and high-end workstation. All these factors cumulatively make WSN vulnerable to internal and external attacks.

Attackers eavesdrop into sensitive message and can inject forged messages into the network. Previously intercepted messages can be used for replay and this leads to compromise of authentic sensor nodes. The adversary may also launch DoS attacks, [13] and path based DoS (PDoS) by introducing false data injection which leads energy

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

depletion in CHs. For Internal attacks, the adversary may attempt to read the data stored in CHs' memories, for example make use of an unauthorized node to read significant data from FN's arbitrarily.

C. Keying Mechanisms

Two different types of keys are used in the proposed method to ensure the confidentiality of messages while sending the message over the network, proposed keys are:

Session keys: This key is used for CH and BS nodes while transmitting packets to FNs.

Pair wise keys: These keys are used for each pair of FNs. Session keys are disseminated before deploying the sensors in the network. After the deployment of sensors, a pair wise keys are generated for every pairs of sensor nodes using CARPY+ scheme [14]. The benefit of this scheme is that without any communication the pair wise keys are established between each pair of sensor nodes, and thus authentication is not required. The complexity of CARPY+ scheme is $\Omega(2^{l+1})$ where l is a parameter of security independent of the number of sensor nodes [8].
It is resilient to large number of node compromise.

IV. IMPLEMENTATION

This section discusses the Modified CFA with AES in OCB mode [3], Synchronized incremental counter for providing protection against DoS, replay and jamming attacks respectively.

A. Security against DoS attack using Modified MCFA

Protecting WSNs against DoS attack using low-cost and flexible mechanism is a primary research challenge. In this paper MCFA algorithm with AES in OCB mode is proposed for DoS resilience [8]. Out of available cipher block chaining, OCB mode seems to represent the state of the art in authenticated encryption modes, largely due to its speed. According to this mechanism, a source node u sense data from environment and send that data to destination node v through a function node. First the packet is encrypted using AES in OCB mode algorithm at the sender side taking the message, (Ku,v) and IV (Initial Vector) as inputs, and generate different cipher text by encryption using E(Ku,v,IV), then computes h(M) hash value. Node u calculates the Message authentication code (MAC) as follows:

$$\mathbf{MAC_u(v,M) = auth_v(v, K_{u,v}, h(M))+n_{u,s}}$$

Where nu,s, is randomly selected from the set [0, ...2r-2-1] used for perturbation. The packet will traverse through multiple paths and reaches the destination v.

Before reaching the destination, the message may pass through intermediate nodes. When a message M arrives at an intermediate node it calculates verification number ver $f_{\in}$ (u, $K_{\in,u,}$ h(M)) and calculates the subsequent verification difference, $VD_{v,u}$, as

$$\mathbf{VD_{\in,u} = | ver\ f_{\in}\ (u, K_{\in,u}, h(M)) - MAC_u(v, M)|}$$

If $VD_{\in,u} \in [0, 2^{r-1}-1]$, then the integrity and authenticity of the packet message M is successfully verified by computing verification polynomial. If it returns true means there is no DoS attack and the packet is forwarded otherwise, the packet message M is not forwarded. The verification process on destination node v is the same as intermediate node.

CFA - Algorithm

Parameters: u is Source node, v is Destination node, Message M, K is secrete key of AES (Kv,u) , IV Initial Vector

Source node u:

1. Calculate the key (Ku,v)
2. Encrypt E(K u,v,IV)
3. Compute hash value h(M)
4. Calculate MACu(v,M)=authv(v,Ku,v h(M))+nu,s
   Where nu,s is randomly picked from {0, ...2r-2-1}
5. Send the packet Message M:=<u,v,M,MACu(v,M)>

Intermediate node ∈

1.Calculate the key (Ku, ∈)
2. Compute hash value h(M)
3.Compute VD∈,u=|ver f∈ (u,K∈,u,h(M)) − MACu(v,M)|
4. *if* (VD∈,u ∈ {0,... 2r−1−1})
   then forward Message
   else drop the message

Destination node v:

1. Calculate the key ($K_{v,u}$)
2. Compute hash value h(M)
3. Calculate V $D_{v,u}$= |ver f_v(u,$K_{u,v}$,h(M)) − MAC_u(v,M)|
4. *if* (V $D_{v,u}$ ∈ {0,... $2^{r-1}-1$})
   then accept the message M
   else drop the message M

B. Security against Replay and Jamming attack using Synchronized Incremental Counter Method

Proposed mechanism makes use of a synchronized incremental counter as an initial vector IV for attaining semantic security. Mainly, the initial vector value is associated with a buffer filter to cleanse the packet. In the case of replay and jamming attack, IV is appended to the packet at the time of transmission. With the synchronized incremental counter, VCM [15] initializes the counter and maintains a counter for synchronization among the sender and the receiver [8]. This is built within each node for initializing the counter. In every node the synchronized incremental counter gets incremented automatically by one per average delay.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Sender Side

- Sender will set the VCM counter value at the time of sending the packet to the recipient.
- The counter gets incremented by one count for each hop and the propagation delay is assumed.

Receiver Side

- Incoming packet reaches the receiver with a propagation delay [16].
- Two checks will be carried out after successful receive of a packet;

First it determines whether the packet is a valid and secondly it verifies whether the packet has suffered from an attack.

The receiver receives a packet with expected propagation delay, if there is no incidence of jamming attack and when packet do not suffer from attack, VCM counter value is verified to check the replay attack.

V. EXPERMIENTAL RESULTS AND ANALYSIS

The efficiency of the proposed scheme is evaluated through simulation. In this section, our experimental results are illustrated for these algorithms.

A. Simulation Environment

Simulation is performed using JProwler and JFreechart by considering varying number of nodes and malicious nodes in the network. The proposed mechanism is evaluated using three different metrics viz. communication time, energy consumed and packet loss.

Packet loss: Packets gets dropped in the network due to overload or unavailability of communication channel. Packet loss is typically due to congestion in the network. Packet loss is the difference of number of packet sent by the sender and Packet received by the recipient

Packet Loss= (Number of Packet sent) - (Number of Packet received)

Communication time: Total time taken for the packet to traverse from source to destination node.

Communication time= (Time of packet received) - (Time of packet sent)

Energy consumption: Amount of energy consumed to transmit data from source to destination

Energy = Power * Time

Initially, Sensor nodes energy is set to 20 Joules and Function nodes with 60 Joules Energy consumption is the difference of available energy in Sensor node and Function node upon receipt of packet at the destination.

The relevant parameters and their associated values are in listed Table II.

TABLE II
SIMULATION BACKGROUND

Parameters	Value
Number of Nodes	50-100
Sensor node energy	20J
Function node energy	60J
Network area	800*600 mm
Communication range of sensor node	200 Hertz
Communication range of Function node	Greater than 200 Hertz
Base station location	Center

B. Performance Evaluation

This section includes the experimental results analyzed for the parameters communication time, Packet loss and Energy consumption in case of No attack, DoS, Replay and Jamming attacks.

The experimental graphs help us to study the effect of DoS, Replay and Jamming attack. It is observed that, the DoS attack incurs more damage to network with respect to communication time, packet loss and energy consumption parameters. In DoS Attackers' can flood the network with false message that exhaust the communication bandwidth, which in turn degrade the network performance leading to enormous packet loss. The damage caused by Jamming attack is less compared to DoS, but it has more impact than Replay attack. In Jamming the attacker send high intensity radio signals with an intention of targeting legitimate nodes. Finally, the effect of Replay attack is less compared to other two attacks. In replay attack the attacker repeatedly forward the packets and this exhaust the buffer and degrade the network performance.

Fig. 3 shows the performance of the various attacks with respect to communication time by varying the number of nodes. The communication time is directly propositional to number of nodes and increase when there is an attack in the network.

In case of DoS attack communication time will be more as the traffic in the network increases that results in packet loss and nodes have to resend the packets.

The result of packet loss ratio with increase in the number of nodes and attacks are observed in Fig. 4. It is observed that packet loss is almost zero in case of no attack and occurrence of packet loss will be more at the time of attack. When there is attack, there is more traffic which leads to congestion in the network, thereby packets are dropped.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

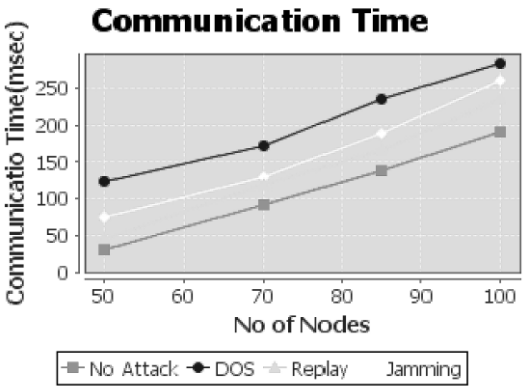

Fig. 3. Graph for communication time v/s number of nodes

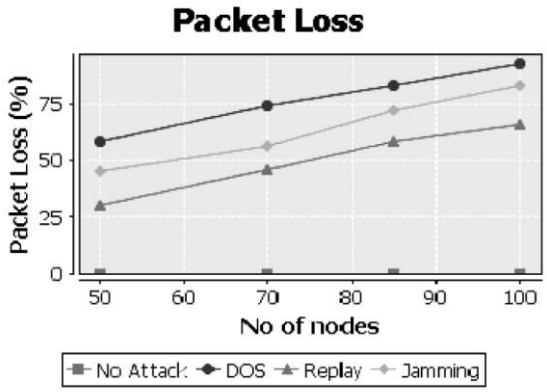

Fig. 4. Graph for packet loss ratio v/s number of nodes

Fig. 5 shows the graph of energy consumption with varying number of nodes. As the number of nodes increases, energy consumption increases as there will more transmission and reception of packets by sensor nodes. Energy consumption is high at the time of attack and considerably low at the time of no attack. This is due to more transmissions, increased congestion and packet loss, there by more retransmission of packets and thus results in more energy consumption.

The Proposed collective method addresses all these attacks. With No attack, the resources like energy and bandwidth is efficiently utilized, thereby increasing the performance of the network and the lifetime of the network.

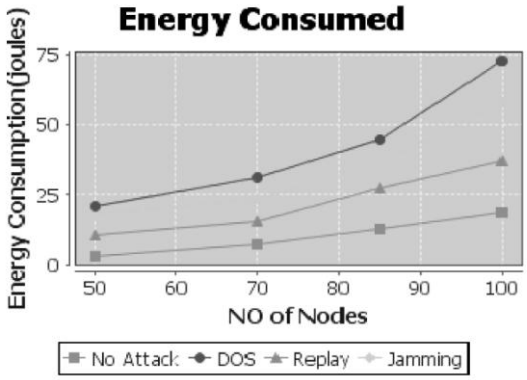

Fig. 5. Graph for Energy consumption v/s number of nodes

VI. Conclusions

Security in sensor networks is a vital area of research. Because of resource limitation and nature of deployment, WSN are more vulnerable to different types of attacks. Among all attacks, DoS attack is considered as most common and critical attack in WSN. In this paper, a security mechanism is proposed to overcome DoS attack and other two major attacks in WSN such as jamming and replay attacks. AES with OCB mode encryption algorithm plays crucial role in providing network layer security, which provides both confidentiality and authenticity at the same time with low energy consumption. The proposed collective methods effectively provide security against all three discussed attacks without degrading the network performance with less packet loss and communication time, thereby increasing the network life time.

References

[1] Rajkumar, Sunitha K R and Dr. H.G.Chandrakanth, "A Survey on Security Attacks in Wireless Sensor Network", International Journal of Engineering Research and Applications (IJERA), vol. 2, iss. 4, July-August 2012, pp.1684-1691.

[2] Aashima Singla and Ratika Sachdeva," Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, iss. 4, April 2013.

[3] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, and Sy-Yen Kuo," Constrained Function-Based Message Authentication for Sensor Networks" IEEE Transactions on Information Forensics and Security, vol. 6, NO. 2, June 2011.

[4] A.Perrig, R.Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," International Conference on Mobile Computing and Networking, 2001, pp.189–199.

[5] *C.Karlof,, N.Sastry, and D.Wagner, "TinySec: a link layer security architecture for wireless sensor networks,"* International *Conference on Embedded Networked Sensor Systems, 2004, pp. 162–175.*

[6] ZigBee Alliance, Zigbee specifications, Technical Report Document 053474r06, 2005.

[7] M.Luk, G.Mezzour, A.Perrig, and V.Gligor, "MiniSec: a secure sensor network communication architecture," International Conference on Information Processing in Sensor Networks", 2007, pp. 479–488.

[8] Yao-Tung Tsou, Chun-Shien Lu, and Sy-Yen Kuo, "MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks", IEEE Transactions on Wireless Communications, vol. 12, No. 6, June 2013.

[9] Kui Ren andWenjing Lou and Yanchao Zhang, "LEDS:Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks", Mobile Computing, IEEE Transactions, volume Voloume: 7, Issue: 5, page 585, May 2008.

[10] Chia-Mu Yu, Yao-Tung Tsou and Chun-Shien Lu, " Constrained Function-Based Message Authentication for Sensor Networks", IEEE Transactions on Information forensics and security, vol. 6, No. 2, June 2011.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[11] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini, Giuseppe Anastasi, and Sajal K. Das, " JAMMY: A Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs", IEEE Transactions on dependable and secure computing, vol. 14, No. 4, August 2017.

[12] Kamal Beydoun, Violeta Felea, “Wireless Sensor Networks Routing over Zones”, Author manuscript, published in SoftCOM 2010, 18th Int. Conf. on Software, Telecommunications and Computer Networks, Croatia

[13] C K Marigowda and Sunanda Golgeri, “Analysis of security mechanisms against Denial-of-Service attack in wireless sensor networks”, Elixir Network Engg, 2014.

[14] C. M. Yu, C. S. Lu, and S. Y. Kuo, “Non-interactive pairwise key establishment for sensor networks,” IEEE Trans. Inf. Forensic and Security, vol. 5, no. 3, pp. 556–569, 2010.

[15] J. J. Hwang, B. M. Shao, and P. C. Wang, “A new access control method using prime factorization,” The Computer, vol. 35, no. 1, pp. 16–20, 1992.

[16] SmartRF, SmartRF CC2420 Datasheet (rev 1.3). Available: http://www.chipcon.com/files/CC2420, Data Sheet 1 3.pdf, 2005.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)