Identifying Selective Forwarding Attacks in Wireless Sensor Networks using multiple resources

K.S.N.V. SOMESWARA RAO

Assistant Professor, Department of Electronics and Communication Engineering, Dadi Institute of Engineering and Technology, Anakapalli, Jawaharlal Nehru Technological University Kakinada

Abstract: *A Wireless Sensor Network (WSN) consists of distributed an autonomous devices that monitors both physical and environmental conditions. Sensor Networks are used for weather prediction and measuring temperature, sound, wave, vibration, pressure etc. Sensor Networks suffer from various security attacks such as sink hole attack, black hole attack, wormhole attack and selective forwarding attacks. Selective forwarding attack happens in compromised nodes by dropping packets selectively. This paper surveys various techniques for detecting selective forwarding attacks in WSNs. A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, hardware, and system constraints.*

Keywords: Wireless Sensor Network, Selective Forwarding Attacks, Compromised Nodes, CHEMAS Technique.

1. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, a radio, and an actuator.1 A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication to transfer the data to a base station (e.g., a laptop, a personal handheld device, or an access point to a fixed infrastructure). Battery is the main power source in a sensor node. Secondary power supply that harvests power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed. Depending on the application and the type of sensors used, actuators may be incorporated in the sensors [1].

Wireless sensor network is a self-configuring network of small sensor nodes which communicates with each other using radio signals. WSN joins together sensing, computation and communication in a single device called as sensor nodes. Wireless sensor nodes are also called as motes. In WSN, sensor nodes are used to send packets to a base station with the help of multi-hop transmission. Sensor nodes are classified into clusters and each of these clusters has a cluster head, it's shown in Fig1. Through cluster heads, Sensor nodes communicate data to the base station by combining data from its members [2].

Wireless Sensor Networks are used in ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, vehicular movement etc. Due to resource constraints of energy and memory, the conventional security measures are not suitable to these wireless sensor networks. An adversary can compromise a sensor node, it alters the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resources. Unlike wired networks, wireless nodes broadcast their messages to the medium. In wired network, there will not be any security problem but not so with Wireless network [3] .

Attacks against wireless sensor networks could be broadly considered from two different levels of views.

1. The attack against security mechanisms.
2. The attack against routing mechanisms.

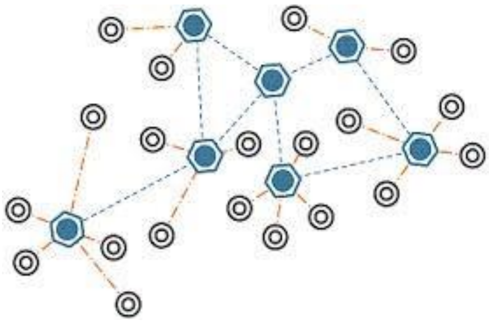

Figure 1: Wireless Sensor Network

Attack Models

Several security attacks exist in Wireless Sensor Networks and they are,

1. Dos attack
2. Sink hole attack
3. Black hole attack
4. Wormhole attack
5. Selective forwarding attacks.
6. Sybil attacks
7. Sybil attacks
8. Node replication attacks
9. Hello flood attack

The main objective of this paper is to give an overview for researchers and developers on different techniques available to prevent Selective Forwarding Attack. This paper is organized as follows: Section 2 present the overview of selective forwarding attack and its types. Section 3 classifies the previous works on Selective Forwarding Attack. Section 4 gives the future research directions. The final section concludes this paper.

2. RELATED WORK

Selective Forwarding Attack

The selective forwarding Attack was first described by Karlof and Wagner [3]. Selective Forwarding Attack is a network layer attack [2]. In this type of the attack compromised nodes drop particular sensitive messages and forward the rest. It is difficult to identify the compromised node in the whole network.

Selective forwarding attacks are most effective when the attacker is explicitly included on the path of a data flow. Selective forwarding and black hole attacks are very disastrous attacks for sensor networks if used with sinkhole attack because the intruder can drop most of the important packets. Further classification of this attack is inside attack and outside attack. Inside attack occurs within the network through compromised nodes and outside attack occurs from outside of the network by jamming the communication channels between uncompromised nodes [4] .

Different Forms of Selective Forwarding Attack There are different forms of selective forwarding attack. In the First form of the selective forwarding attack, the compromised node drops some packets. In its Second form, the Selective forwarding attack behaves like a Black hole, in which the message is forwards to the wrong path, creating false routing information in the network. Third form of selective forwarding attack delays packet passing through the network creating confused routing information between sensor nodes [3].

3. RELATED WORK

Various techniques are introduced by several researchers to detect malicious nodes that cause selective forwarding attack in Wireless Sensor Networks. These techniques are classified and depicted below in fig 2.

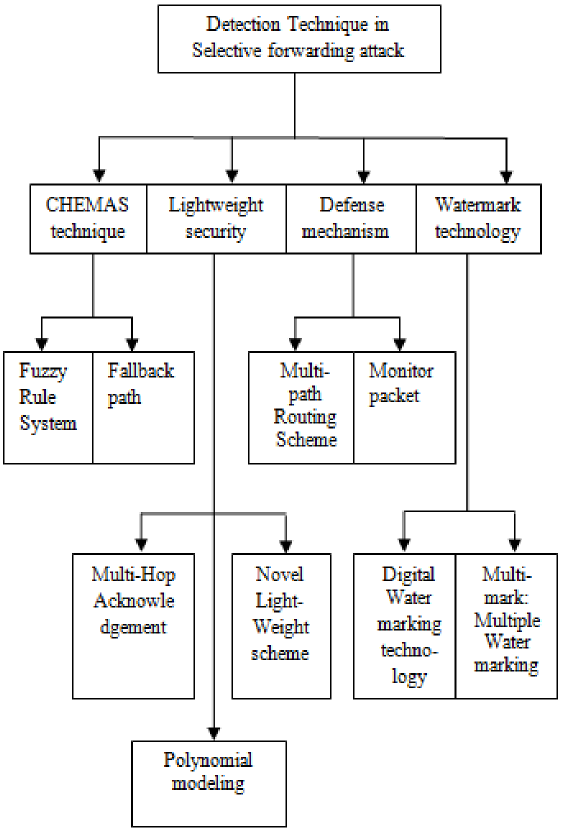
Detection Technique in Selective forwarding attack
CHEMAS technique
Lightweight security
Defense mechanism
Watermark technology
Fuzzy Rule System
Fallback path
Multi-path Routing Scheme
Monitor packet
Multi-Hop Acknowledgement
Novel Light-Weight scheme
Digital Water marking techno-logy
Multi-mark: Multiple Water marking
Polynomial modeling

Figure 2: Classification of Selective Forwarding Attack Techniques

Applications

WSN applications can be classified into two categories: monitoring and tracking Monitoring applications include indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans, and vehicles. While there are many different applications, below we describe a few example applications that have been deployed and tested in the real environment.

CHEMAS Technique

The Checkpoint Based Multi-hop Acknowledgement Scheme (CHEMAS) was proposed by Bin Xiao et al., to detect selective forwarding attack. When message is generated by a source node and is delivered to the base station, the checkpoint nodes are selected randomly. The base station and each checkpoint nodes generate acknowledgement (ACK) message that is transmitted from the start node to the source node [5]. ACK messages have the Time to Live (TTL) value, which sets the hop count. If TTL becomes zero, ACK message is dropped and an alert message is sent to the source node. If a particular node does not send ACK message to the source then it is identified as the compromised node. Then the source node sends an alarm message about the compromised node to the base station.

Ji Won Kim, et al., [5] in their research work, have proposed another technique for the Checkpoint Based Multi-hob Acknowledgement Scheme (CHEMAS) to detect the compromise nodes that perform a selective forwarding attack when sensing data transmission. This paper has achieved a higher detection ratio through each checkpoint node and it generates acknowledgement message to confirm the normal packet. However, if more number of check nodes is presented, then the checking time of the packet transferred will increase and so there will be a time delay in reaching the destination.

Ji Won Kim, et al., [4] in their work, have presented a control method of checkpoint node selection using a fuzzy rule system and feedback in the Checkpoint Based Multi- hob Acknowledgement Scheme (CHEMAS). The sink node and each checkpoint node generate acknowledgement (ACK) packets to confirm normal packet delivery. If a node has not received sufficient ACK packets, then the nodes generates an alert packet to report the suspect node. Compromised nodes can be detected by analyzing the alert information reported. However, it increases communication.

Defense Mechanism

Defensive technique for selective forwarding attack consists of three phases for secure information delivery. In first phase the node discovers a path and its neighbor nodes, in second phase, data is propagated in multipath, it checks whether the data received is correct or not, and in the final phase if any error is detected then a MONITOR packet is generated and the malicious node is removed.

Geethu P C and Rameez Mohammed A., [4] in their research work, have described a multipath routing scheme that is used as defense mechanism against selective forwarding attack. When a node detects packet drop during the routing, it will resend the packet through alternate route, as the resending mechanism reliability of the routing scheme improves then Packet is retransmits through another alternate path. If that path is busy with some other transaction, it leads to time delay and there is a chance for jamming and this is the Limitation of this work.

Pandarinath P., [1] in his research work, has given defensive technique for selective forwarding attack in localization. This technique utilizes secret sharing of information and this information is shared between source and destination using secret sharing algorithm. This algorithm is not suitable for all situations. This algorithm takes more time to execute when more nodes are participating. Arpita Parida, et al., [4] have introduced a Defensive technique, if any attack is encountered then a monitor packet is generated and subsequently the malicious node is removed. It finds a new path so that the connection will not to be lost and also good delivery ratio can avoid delays. When the path increases, the energy consumption also increases simultaneously.

Lightweight Defense Scheme

Lightweight security scheme is used to detect selective forwarding attack using multi hop acknowledgement technique. This scheme allows both the base station and source nodes to collect attack alarm information from intermediate nodes. In other words, though the base station is deafened by malicious node the source node can make decisions and responses. The scheme can efficiently obtain those alarm information whenever intermediate nodes in a packet forwarding path detect any malicious packet dropping.

Wang Xin-sheng, et al., [6**]** in their research work, have proposed a light weight defense scheme against selective forwarding attack which uses neighbor nodes as monitor nodes. The neighbor nodes (monitoring nodes) monitor the transmission of packet drops and resend the dropped packets using a hexagonal WSN mesh topology. Limitation of this paper is that if there is any change in topology, it will affect the performance of the scheme as it is assumed that after development the nodes will not change their location.

Xie Lei et al., [5] in their research work, have described polynomial modeling based on countermeasure against selective forwarding attack and a security scheme using redundant data to tolerate the loss of messages. The basic idea is to split the original data into small parts and forward these parts to the base station. Forwarding nodes cannot understand the contents of the data generated by the polynomial, which can prevent eaves dropping and so sensor nodes in the network cannot be compromised. Finally, before the sensor nodes are deployed, every node shares a unique symmetric key with the base station. However, dividing and processing the original data packet into small sizes leads to extra storage [8].

Watermark Technology

The digital watermarking technology is used to calculate the rate of packets of dropped and modified. Each sensor node can send only a few bits at a time and so the length of watermark embedded into the data should be very short. The source node generates the watermark W with key K and the feature of the original data. Then the source node embeds the watermark into the original data and transfers it through the media. When the packets reach the Base Station, it the Base Station obtains the feature of the packets and generates the watermark W1 by watermark generation algorithm, then the Base Station extracts the watermark directly from the received packets by Watermark embedding algorithm denoted as W2; finally the packet modified rate is calculate by comparing the W1 and W2.

Deng-yin ZHANGa, et al., [6] in their research work, have presented a technique based on digital watermarking technology. This method embeds watermark into the source data packets, and extracted them at the base station without any packet loss. The malicious node prevented from dropping the data. The limitation of this scheme is that it cannot detect more than two malicious nodes on the single path.

Baowei Wang, et al., [7] in their research work, have proposed a novel multiple watermarking method called Multi-mark. This technique provided privacy, security, and saved storage space and the amount of data transmitted. Multi-mark is a network structure-free scheme, which can be easily and efficiently applied to the resource limited sensor networks.

4. Future Research Directions

In the existing Defensive technique algorithm, asingle static path is created for sending packets to the sink node in the network. When an attack is identified, server removes the malicious node and the packets are retransmitted through the new shortest path without losing the connection. This technique can be further enhanced by hiding the packets using the secret sharing algorithm. This approach leads to less conception of energy, good delivery ratio and avoids delays.

Research in WSNs aims to meet the above constraints by introducing new design concepts, creating or improving existing protocols, building new applications, and developing new algorithms. In this study, we present a top-down approach to survey different protocols and algorithms proposed in recent years. Our work differs from other surveys as follows:

- While our survey is similar to [1], our focus has been to survey the more recent literature.
- We address the issues in a WSN both at the individual sensor node level as well as a group level.
- We survey the current provisioning, management and control issues in WSNs.
- These include issues such as localization, coverage, synchronization, network security, and data aggregation and compression.
- We compare and contrast the various types of wireless sensor networks. Finally, we provide a summary of the current sensor technologies.

5. Conclusion

The Checkpoint Based Multi-hop Acknowledgement Scheme (CHEMAS) technique is very effective technique for malicious node detection to compare with any other techniques. In CHEMAS, the selection probability of checkpoint is an important factor to determine the security intensity and energy efficiency. The proposed method enhances detection ratio with similar energy consumption to the original CHEMAS scheme. Secure transaction is very difficult in wireless sensor network. This paper surveys various effective detection techniques for selective forwarding attack in WSN, proposed by various researchers. This analysis will facilitate to know the drawbacks in the earlier schemes and will help to overcome the drawbacks in the future.

References

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghoshal,"Wireless sensor network survey", www.elsevier.com/locate/comnet, April 2008, pp. 2292–2330

[2] Chris Karlof and David Wagner," Secure routing in wireless sensor networks: attacks and countermeasures in Ad Hoc Networks", www.Elsevier.com, Vol.1 No.2, September 2003, pp.293–315.

[3] Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalem,Quratulain Arshad," The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures" International Journal of Wireless and Microwave Technologies (IJWMT), Vol.2, No.2**,** April 2012, pp.33-44

[4] Y. Sankarasubramaniam, O.B. Akan, I.F. Akyilidiz, ESRT: event-tosink reliable transport in wireless sensor networks, in: Proceedings of the MobiHoc, Annapolis, MD, 2003.

[5] C.-Y. Wan, S.B. Eisenman, A.T. Campbell, CODA: Congestion detection and avoidance in sensor networks, in: Proceedings of the Sensys, 2003.

[6] K. Seada, M. Zuniga, A. Helmy, B. Krishnamachari, Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks, in: Proceedings of the Sensys'04, Baltimore, MD, 2004.

[7] R. Zhang, H. Zhao, M.A. Labrador, The anchor location service (ALS) protocol for large-scale

wireless sensor networks, in: Proceedings of the First International on Integrated Internet Ad hoc and Sensor Networks, Nice, France, 2006.

[8] J. Yin, S. Madria, SecRout: a secure routing protocol for sensor networks, in: Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), Vienna, Austria, 2006.

Author's Profiles:

K.S.N.V.SOMESWARA RAO working with as Assistant Professor, Department of Electronics and Communication Engineering in Dadi Institute of Engineering & Technology (DIET) - Anakapalli, affiliated with Jawaharlal Nehru Technological University-Kakinada. He is completed AMIE in ECE from Institution of Engineers of India (IEI), Kolkata. He is completed in Master Degree in Embedded Systems from Jawaharlal Nehru Technological University-Kakinada, Andhra Pradesh, India.

He has 4 years Industrial and 13 years good teaching experience with taught various subjects on good knowledge on EDC, Microcontrollers and Applications, Microprocessor and Interfacing, Electronic Circuit Analysis, Embedded Systems, EMWTL, Signals and System along with ECE subjects. He has honored IET Professional Member National Level Award in 2013 and published 5 research papers in reputed International and national level conferences\Journals\Magazines. He has attended 2 conferences, 6 workshops. He is the member of IEEE, IAENG, AMIE and IET. He is Participated and active member in academic, curriculum and administrative works in various organizations.