IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Vulnerabilities of Routing Protocols in Wireless Sensor Networks

Celia John[1], Charu Wahi[2]

Student, Birla Institute of Technology, Mesra, India[1]

Assistant Professor & Coordinator, Birla Institute of Technology, Mesra , India[2]

Abstract*:* The demand for WSN is increasing day by day and in the deployment of WSN the most challenging issue faced is its security. Hence, there is a necessity to design and develop new secure routing solutions for WSN. This research paper discusses about different security attacks like Selective forwarding, Sinkhole, Sybil and blackhole with their impact on the Routing protocols. The effect of these attacks has been summarized. This article emphasizes on reviewing the effects of network layer attacks on Routing protocols in WSNs. A table has been presented summarizing the same.

Keywords: WSN, Routing, Security, Attacks, Sensors.

I. INTRODUCTION

Wireless sensor Networks (WSNs) are gaining a lot of attention lately owing to the technology advancements leading to highly integrated digital electronics. With the development of the electronic industry and semiconductors in particular, it has been possible to develop low cost, low power, integrated sensors. The built in functionality in the sensors have increased tremendously and this has lead to the development of Wireless sensor networks which aids in data processing, storage and communication of information.

Wireless sensor networks are a network of thousands of sensors distributed in a region in order to serve a purpose. The information from the sensors is sent using multi hop to a central gateway or a user for sending to other networks. The sensors operate under severe resource constraints with limited compute power, memory and bandwidth. Deployment of these sensors can happen randomly (using helicopters in risky areas or in disaster management) or manually planted (e.g. Fire detectors in a building). The applications vary widely from Weather prediction techniques, military applications, Medical related, monitoring environmental parameters like pressure, temperature, vibration etc. Reliable environment monitoring is an integral part of commercial & military applications. The requirements and needs of WSN make their architecture both challenging and different from the traditional internet architecture.

The remainder of the paper is as follows: Section II contains an overview on Secured Routing, types of attacks on WSN with special focus on the types of attacks on Routing Layers of WSN. Section III gives a comparative evaluation of routing protocol against security attacks. Finally the conclusion highlights the findings of the security analysis done on some Routing protocols.

II. SECURED ROUTING

Routing is required to send data from the sensor nodes to the Base-station or the destination. Routing in WSNs is different from the conventional routing due to the absence of a fixed infrastructure in WSN resulting in compute and communication challenges. In order to be effectively utilized the sensor nodes need to be

- Cost effective (as they are typically deployed in thousands and are not replaceable)
- Limited power (affect lifetime as battery or sensor nodes may not be replaceable)
- Limited computation (due to limited power)
- Operable in hostile environments
- Redundancy (to account for nodes towards end of lifetime)

These constraints drive the routing protocols to be used in Wireless Sensor Networks. Routing Protocols have been classified based on various criteria [1] [2]. One such classification is based on the network structure and is of Flat, Hierarchical and Geographic based routing. An example of Flat routing protocols is SPIN (Sensor Protocols for information via Negotiation). LEACH (Low Energy Adaptive Clustering Hierarchy) and PEGASIS (Power Efficient Gathering in Sensor Information Systems) are examples of hierarchical network structure, whereas GAF (Geographic Adaptive Fidelity) & GEAR (Geographical and Energy Aware Routing) form part of Geographic based routing.

The wireless nature of communication makes WSNs prone to tampering of control and data information which prove to be a disaster in many applications. Use in military applications need critical data to be transferred among the sensors, which if intercepted can prove to be fatal. Similarly in areas where the natural parameters are monitored for potential landslides/earthquakes, the data is crucial for predictions or analysis. Security is essential for both wired and wireless networks, but security in wireless itself differs widely from the wired networks. The existing secured solutions are too expensive and consume a lot of processing time in WSNs. The need for security can be summarized below:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

- Since transport medium in WSN is broadcast in nature, any adversary with a strong receiver can intercept it.
- An adversary can disrupt the network.
- Message alteration can occur.
- Constraints in incorporating security in WSN due to inherent limitations (e.g. increased compute facility/power for implementing high levels of security is not available.)

Here our attempt is to focus on different types of attacks against network layer in WSNs

A. Types of Attacks

Attack in Wireless sensor networks can be classified [3] into two types namely:

- Passive Attacks

These are attacks where the attacker snoops on the network and has access to all the information being sent from one node to the other. The attacker does not modify the contents or the routing information in the data, but can gather information to get authentication information based on which it can launch further attacks e.g. Eavesdropping, Sniffing.

- Active Attacks

In Active attacks the adversary node can modify the information or create fake data streams which could waste energy resources of the network. These attacks can destroy the network and impede the availability of authentic and correct information. Denial of service and replay are some of these types of attacks

These attacks can be initiated by internal or external attackers. Internal attacks occur when a sensor node within the network acts unusually or it has been compromised. In External attacks the attacker eavesdrops on the network to extract information and gain access to it.

B. Routing Layer Attacks on WSN

This section describes the various routing layer attacks on WSN.

1) Selective forwarding

Routing in WSN follows a multi-hop approach where all the information is sent from node to node till it reaches the Base Station or the destination. In case of selective forwarding attack, a compromised node may resort to forwarding only some of the data packets while dropping others. This selective dropping results in loss of data, re-transmission and loss of bandwidth. Fig. 1[4] illustrates selective forwarding attack.

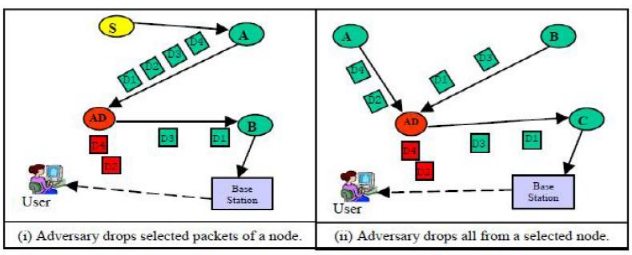

Fig. 1: Selective Forward Attack

2) Sinkhole Attack

Sinkhole attack is characterized by the attacker trying to route all the traffic via a compromised node making it appear to the other nodes as a route which is closest to the destination and therefore the best route for the data. The compromised node advertises about itself and the other nodes thereby route all the information through this node. These attacks can occur in flat & hierarchical routing. In Fig. 2 [4], the SH node indicates the Sinkhole, which routes all the traffic through itself.

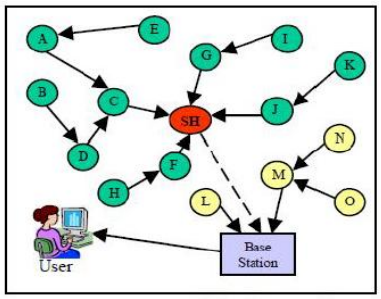

Fig 2: Sinkhole Attack

3) Black hole Attack

In Blackhole a node in the range of the sink makes itself attractive to the other nodes and attracts the entire traffic through itself by advertising as the shortest path. As the other nodes route data through the compromised node, it resorts to dropping of packets from certain sources, thus isolating the node and creating discontinuity in network [4]. Refer to the fig. 3 [4].

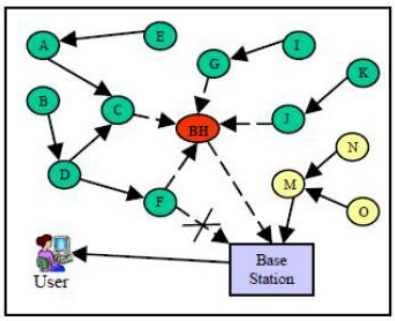

Fig 3: Black Hole Attack

4) Sybil attack

In a WSN the routing protocol assumes that each node has a unique identity. In Sybil attack, a compromised node appears to have multiple legal identities at different times. Multiple identities are possible by creating fake identities at the edge of the communication range.

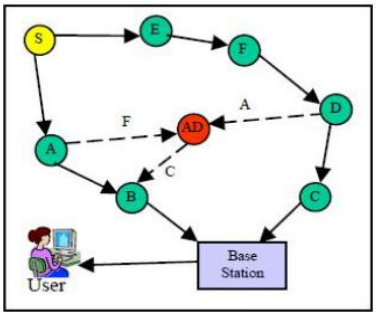

Fig 4: Sybil Attack

DOI 10.17148/IJARCCE.2016.52103

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Sybil attack is a threat to flat routing, hierarchical based routing and geographical routing. The above Fig. 4 [4] demonstrates a Sybil attack where a attacker node `AD' appears as 'F' for 'A', 'C' for 'B' and 'A' as to 'D', When 'A' wants to communicate with F , it sends message to 'AD'

5) Wormhole Attack

Wormhole attack is a severe kind of attack on Wireless Sensor Network Routing where two or more attackers are connected by a high speed link called Wormhole link. In wormhole an attacker could convince the other nodes which are far from the BS, that they are only single hop away from the destination. This results in the neighboring nodes directing data towards the Wormhole, which finally does not reach the destination. This attack combined with selective forwarding and Sybil makes it very difficult to detect it. Fig. 5 indicates a Wormhole attack [5].

Packets received by node X are sent to node Y through the Wormhole. X to Y would normally have taken multiple hops but the attacker makes A & B believe that they are neighbors by forwarding routing messages and dropping data to disrupt communication between them.

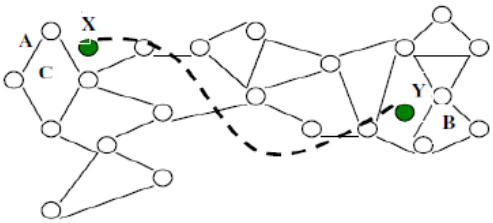

Fig 5: Wormhole Attack

III.COMPARATIVE EVALUATION OF ROUTING PROTOCOLS AGAINST SECURITY ATTACKS

C. Text Font of Entire Document

Blackhole and grayhole attacks on LEACH protocol are compared in [6]. A blackhole attacker tries to collect data from network and finally drops it. In LEACH the cluster heads (CH) are selected based on maximum residual energy. Since attackers are nodes with high energy, the attacker is selected as the cluster head in the first round. Since the attacker does not do any transmission, its energy is preserved and it is selected as a cluster head in subsequent rounds as well. Being a clusterhead, it can aggregate the data and not send it to the Base-station.
An author in [6] shows the impact of gray hole and black hole on LEACH performance. Modification in LEACH protocol was done to form SLEACH to improve security only against outsider attack [7]. SLEACH also protects the network against selective forwarding, sinkhole and HELLO flooding attacks by not allowing the CH to send fake data to the sensor.

In **grayhole attack**, the malicious node advertises itself as the one with the highest chance of being selected as a cluster head. Due to the unpredictable & random behavior it becomes difficult to detect the grayhole attack. Pravin et.al.[8] have compared the performance of LEACH on grayhole attack on the basis of parameters like packet drop ratio, throughput and Average end-to-end delay. With the grayhole attack the PDR dropped from 80% to 77%, while the average end to end delay increased from 4.69ms to 5.17ms. The throughput after attack was 23.11 kbps as compared to 32.06 kbps without the attack.

Wormhole attack detection mechanisms are discussed in [5] which can help recognize a wormhole and avoid it. This is done by the use of directional antennas, if a sender sends packet in one direction the other node should receive it in the opposite direction. Sending and receiving in opposite directions indicates that the nodes are neighboring ones, or else it could be through a wormhole. Another means of identification is by using the message travelling time, from the time the request is made from one node to getting the reply from the destination node. This time is compared with the time for the request reply from the neighboring nodes. If it is larger, it indicates a wormhole transmission.

Hop counting is another means of detecting wormhole attacks. In [9] a strategy of digital investigation of Wormhole attacks is mentioned where a set of investigator nodes are distributed in the network, which run algorithms to identify potential wormhole scenarios.

Sadeghi et.al. [10] mentions that **sybil attacks** are of great danger to geographical routing protocols. In Geographical routing protocol, the location information of the node & residual energy is a decisive factor to choose the next hop. However, using multiple identities in a Sybil Attack, an adversary node can advertise itself with maximum energy. Security mechanism against Sybil attack based on LEACH routing protocol has been discussed in [11]. The mechanism uses a Sybil attack detection policy based on RSSI (Received signal strength indicator). The Sybil node broadcasts with high power, which makes other nodes assume that it is the clusterhead. This node will have different Identities due to which its chances of becoming a cluster head increases resulting in increased chances of broadcasting messages. When the number of cluster heads in the network is over a threshold, it indicates Sybil attack. The mechanism is analyzed for security and energy consumption.

Edith et.al. in [12] present a novel algorithm to detect **sinkhole attacks**. The method involves finding a list of suspected nodes by checking data consistency, and then identifies intruder in the list through analyzing the network flow information. Geographic Routing Protocols are to an extent resistant to Sinkhole attacks [12][13]. Many current routing protocols are susceptible to sinkhole, especially those based on route advertisement.
Algorithms to detect sinkhole attacks are in place and one such algorithm [14] involves finding a group of suspected nodes based on analyzing the data consistency, and then intruder is identified by checking network flow information.

Karlof & Wagner [15] mention why geographic routing can be relatively secure against wormhole, sinkhole and Sybil attacks. However, the location information from the neighbors must be trustworthy. A compromised node can

DOI 10.17148/IJARCCE.2016.52103

indicate that it is the destination for all the forwarded packets and can selectively drop them. Multipath routing can help by selecting multipath routing to multiple base stations.

Various research works have been done in the area of secured routing protocols in WSN. This article emphasizes on reviewing the effect of network layer attacks on Routing Protocols in WSN. A Table has been presented summarizing the same. Refer to Table I given below.

Table I: Summary of Attacks on routing protocols

Routing Protocols	Classification	Attacks					
		Selective Forwarding	Gray Hole	Black Hole	Sybil	Sinkhole	Wormhole
LEACH	Hierarchical	yes	yes	yes	yes	yes	yes
TEEN & APTEEN	Hierarchical	yes	yes	yes	yes	yes	yes
VGA	Hierarchical	yes	yes	yes	yes	yes	yes
PEGASIS	Hierarchical	yes	yes	yes	yes	yes	yes
SPIN	Flat Based	yes	yes	yes	yes	yes	yes
RR	Flat Based	yes	yes	yes	yes	yes	yes
DD	Flat Based	yes	yes	yes	yes	yes	yes
GEAR	Location Based	yes	yes	yes	yes	no	no
GAF	Location Based	yes	yes	yes	yes	no	no

IV. CONCLUSION

We see that the various routing attacks affect all the types of Routing- Flat, hierarchical and Location based. This impact can be reduced by using countermeasures for each of the attacks. Minor changes in the protocol can help in making it resistant to attacks. However, due to the severe resource constraints, complex computations cannot be implemented in the tiny sensors as they can greatly reduce the network lifetime.

REFERENCES

[1] Rajashree.V.Biradar, V.C .Patil, Dr. S. R. Sawant, Dr. R. R. Mudholkar, ”Classification and Comparison of Routing protocols in Wireless sensor Networks”,Ubiquitous Computing Security Systems,2009

[2] Subhajit Pal,Debnath Bhattacharya, Geetam S. Tomar,Tai-hoon Kim, “Wireless sensor networks and its Routing Protocols: A Comparitive Study” International conference on computational Intelligence, 2010

[3] Nusrat Fatema,Remus Brad,”Attacks and counter attacks in Wireless sensor Networks”, International Journal of Ad-hoc, Sensor & Uiquitous Computing, Dec 2013

[4] Jyoti Shukla, Babli Kumari, “ Security threats and defense approaches in Wireless sensor networks – An Overview”, International Journal of Appplication or Innovation in Engineering and Management, 2013

[5] Meenakhi Tripathi, M.S.Gaur ,V. Laxmi,”Comparing the attack of Blackhole & Gray hole attack on LEACH”, Science Direct 2013

[6] Priya Maidamwar,Nekita Chevhan, “A survey on security issues to detect wormhole attack in wireless sensor network” 2012

[7] Bhakti Parmar, Jayesh Munjani, Jemish Meisuria, Ajay Singh,”Survey of routing protocol LEACH for WSN”, International Journal of Scientific and Research Publications , 2014

[8] A. Pravin Renold, R. Poongothai, R. Parthasarathy,” Performance Analysis of LEACH with grayhole attack on Wireless Sensor Networks”.2012 International conference on computer Communication and Informatics

[9] Bayrem Triki,Slim Rekhis, Noureddine Boudriga,” Digital investigation of Wormhole attacks in Wireless Sensor Networks”.2009 Eighth IEEE International Symposium on Network Computing and Applications

[10] Mohammad Sadeghi,Farshad Khosravi,Kayvan Atefi, Mehdi Barati; “Security Analysis of Routing Protocols in Wireless Sensor networks”,IJCSI Jan 2012

[11] Shanshan Chen , Geng Yang, Shengshou Chen, “ A Security Routing Mechanism against Sybil attack for wireless sensor networks”, 2010 International conference on Communications and Mobile Computing.

[12] Edith C H Ngai, Jiangchuan Liu, Michael R Lyu;”On the intruder Detection for Sinkhole Attack in Wireless sensor networks”,2006

[13] Tejinderdeep Singh, Harpreet Kaur Arora;”Detection and Correction of Sinkhole Attack with Novel Method in WSN using NS2 Tool”,IJACSA,Vol4, No.2 , 2013

[14] Ahmad Salehi, M.A. Razzaque, Parisa Naraei, Ali Farrokhtala; “Detection of Sinkhole attack in Wireless Sensor Networks”2013 IEE International Conference on Space Science and Communication , July 2013, Melaka Malaysia

[15] Chris Karlof, David Wagner;”Secure Routing in Wireless Sensor Networks : Attacks and Counter measures”, Special Issue in Sensor Network Applications and Protocols (2-3) (2003) 1293-1303