International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 3 ISSUE 2 (2018) PAGES 161 - 168

Received: 20/02/2018. Published: 22/03/2018

SURVEY ON WIRELESS SENSOR NETWORKS

N.Suma, S.Yamini Priya,V.S.Kanimozhi
Department of Electronics and Communcation Engineering
Dhanalakshmi Srinivasan College of Engineering Coimbatore, India.
Email: kalai_suma@yahoo.com

ABSTRACT

Wireless sensor network (WSN) is an emerging field. A multitude of WSN exist today in various fields, each having specific objective in mind. From application areas of WSN, it has been observed that one of main important constraints in WSN is Security. Information in the network must be protected from the attackers. Security and privacy to small sensor nodes is challenging due to the limited capabilities of sensor node in terms of computation, communication, memory/storage and energy supply. This paper aims to survey the state of the art in research on wireless sensor network security and highlights their key features, including strength and weakness.

Keywords: - Routing Attacks, Routing Protocols, wireless sensor networks.

I. INTRODUCTION

some security mechanisms applied in A wireless sensor network consists of densely deployed sensor node. These nodes incorporate wireless transceivers so that communication and networking are enabled. Ideally, individual nodes should be battery powered with long lifetime and should cost very little. Furthermore, security requirements are needed in a secure network to ensure the protection and safety of data and systems involved. This provides, stronger and complete protection against illegal activities maintaining at the same time the stability of the system. In this paper, WSN are analyzed. The rest of the article is organized as follows. In section II, outline design and development of wireless sensor network is outlined. Next, some existing security mechanisms of routing attack for WSN is reviewed in section III. In section IV, various routing protocols and attacks in WSN are discussed. Finally, the conclusions and prospect of this paper are given.

II. DESIGN AND DEVELOPMENT OF WSN

The WSN consists of sensor nodes which are used for sensing, processing and communication purposes. Each sensor node senses any kind of physical parameter depending upon the need of users and this measured parameter is transformed into electrical signal. The signal is further processed and transmitted to other nodes as each node has the capability to communicate with each other or directly to the base station. A WSN contains hundreds to thousands of sensor nodes. A greater number of sensors allows for sensing over larger geographic regions with greater accuracy. Basically each sensor node comprises sensing, processing transmission, mobilizer, position finding system and power units. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor node coordinates among them to produce high quality information about the physical environment. A base station is typically a gateway to another network, a powerful data processing or storage center or an access point for human interface. The base station receives a steady stream of data from sensor nodes. However sensors are constrained to use low-power, lower bandwidth, shorter range radios.Ishizuka [16] et al proposes three strategies to deploy sensors (simple diffusion, uniform density deployment and random deployment) and compares their performance on sensing rate, routing rate and transmission rate. To reduce the total numbers of message sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points.

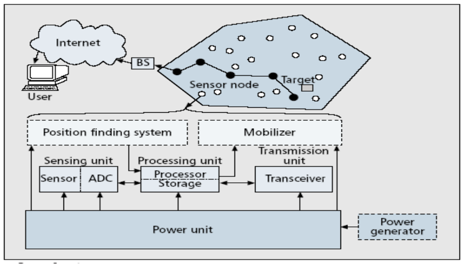


Figure 1. Architecture of WSN

Aggregation points are typically regular sensor nodes and their selection is not necessarily static but can be chosen as dynamic for each query. The network use wireless communication which is assumed that radio links are insecure. Secure routing protocol should guarantee the integrity, authentication, confidentiality, secure management.

III.ROUTING ATTACKS IN WSN

WSN is more vulnerable. The main threats include interception, interruption, modification and fabrication. The attacks on routing will threat the security of the sense data directly. Generally, secure routing protocol in WSN should be efficient in energy consumption. It must be sensitive and extensible. Many of the algorithms have been proposed for the problem of routing data in WSN. Many sensor network routing protocols are quite simple, and for this reasons are sometimes even more susceptible to attacks against routing protocols Karlof [3]. Most network layer attacks against WSN are

Spoofed, or replayed routing information.
Selective forwarding
Sinkhole attacks
Sybil attacks
Wormholes
HELLO Flood attacks.

A. Spoofed or replayed routing information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering or replaying routing information, adversaries may be able to create routing loops, generate false error message, and partition the network. An unprotected routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information. Here, attacker can create loops, attract or repel

Received: 20/02/2018. Published: 22/03/2018

network traffic, generate false message, partition network, and induce delay. This can enable an attacker to create routing loops in the network or to increase the length of resources Karlof [3].This in turn causes increased traffic congestion and deprives the network.

B. Selective forwarding

Multihop networks are often based on the assumption that participating nodes will faithfully forward received messages. In selective forwarding attacks, malicious node may refuse to forward certain message and simply drop them, ensuring that they are not propagated further. This type of attacker runs the risk that neighboring nodes will conclude that it has failed and decides to seek another route.

Attacks: They can corrupt a number of existing routing protocols such as TinyOS beaconing, Directed diffusion, GPSR, GEAR and cluster based protocols, especially when they are used in combination with other attacks such as wormhole and sinkhole. The attack can be used to make a denial of service attack targeted to a particular node. If all packets are dropped, the attack is called a “black hole”.

Defenses: Karlof [3] suggested countering selective forwarding by using multipath forwarding. But it has drawbacks which are communication overheads, increase dramatically as number of paths increases, poor security resilience. Bo yu [20] presented the design of Multihop acknowledgement-based detection scheme in which both the base station and source nodes have the capability to detect this attack.Yu and Xiao [21] proposed a scheme in which both base station and sensor nodes have the responsibility to defend against this attack. But it has some drawbacks which are sensor nodes take much effort to detect this attack, lack of scalability. The multi data flow topologies(MDT)scheme [22]defend against selective forwarding .The main advantage of this scheme are base station can receive information sensing from sensor nodes continuously, light weight, simple and can defend several kinds of attacks.

C. Sinkhole attack

An important form of routing attack is sinkhole attack [3].In this attack, a malicious node falsely advertises that it has a low hop-count route to the base station.

Attack: Many-to-one communication is highly vulnerable to sinkhole attack. A sinkhole attack prevents the base station from obtaining complete and correct sensing data and thus forms a serious threat to higher-layer applications.

Defenses: Redundancy or random selection is most efficient mechanism defending against sinkhole attack, location aware mechanism also suppress this attack. In probabilistic routing, nodes dynamically select next hop in a certain probability. Then every neighboring node has chances to be selected as next hop, which will reduce the chance of sinkhole attacker to control all the dataflow. In geographic routing [8] every node establishes their path to sink by their physical location. To detect sinkhole attack intrusion detection system (IDS) that recognizes abnormal route updates. Daniel [15] presents an anomaly detection scheme (ADS) to detect abnormal route advertisements that are caused by sinkhole attacks and applicable to any routing protocol. ADS analyses the magnitude of hop-counts stored in node’s routing table, using single ADS detection rate of 96% is achieved.

D. Sybil attack

All multi path routing protocols are vulnerable to Sybil attacks. The malicious node present in the network may advertise different identities. Sybil attack can fool the protocol giving a picture of existence of different routing paths to destination but it is the same path through Sybil node. Attacks: The attacks are Douceur [2] described Sybil attack in the context of peer-to-peer networks. He pointed out that it could defeat the redundancy mechanisms of distributed storage system. Karlof [3] noted that Sybil attack poses a threat to routing mechanism in sensor network.

Defenses: The defenses against this attack are Douceur [2] proposes resource testing as a method of direct validation. The verifier tests whether identities correspond to different physical entities by verifying that each identity has as much of the tested resource as a physical device. This method is unsuitable for wireless sensor network because all the replies converging at the verifier will result in that part of the network becoming congested. The intuitional counter measures to defend against Sybil attack are to prevent any node from forging illegitimate identities. James Newsome et al [6] has proposed radio resource testing, verification of key sets for random key predistribution registration and position verification to defend against Sybil attack. But these methods rely on either strict physical assumptions or cooperation between a bunch of nodes.

E.Wormhole attack

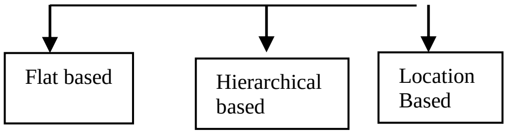
In wormhole attack [3], adversary construct a fake connection and tunnels messages from one side of this fake connection to another slide and then replays them into network locally. It is very dangerous for WSN routing protocols, because attackers even doesn't compromise any sensor node in the network and even all of sensor node utilize effective authentication and confidentiality mechanism, two malicious nodes can collide to form wormhole attack. The defenses against this attack are traffic directed towards base station and not elsewhere.

F.HELLO flood attack

In a HELLO Flood [3] attack a malicious node can send, record or replay HELLO-messages with high transmission power. It creates an illusion of being a neighbor to many nodes in the networks and can confuse the network routing badly. This type of attack attacks the protocols which depend on localized information exchange between neighboring nodes for topology maintenance of flow control is subject this attack. The simplest defense against this type of attack is to verify the bidirectionality of a link. The identity verification protocol verifies the bidirectionality of a link between two nodes and a trusted base station that limits the number of verified neighbors for each node. Restricting number of nodes by the base station will still prevent this type of attack.

IV ROUTING PROTOCOLS IN WSN

Routing in sensor network is a challenge work because of several characteristics that set them apart from conventional networks.



Received: 20/02/2018. Published: 22/03/2018

Figure2.Classification of routing Protocols

All the routing protocols are classified as flat based routing protocol which performs the operation of sensing task and multihop communication based upon flooding. Hierarchical protocols aim at clustering the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location-based protocols utilize the position information to relay the data to the desired regions rather than the whole network. Data-centric protocols are query-based and depend on the naming of desired data, which helps in eliminating many redundant transmissions All proposed protocols are susceptible to attack. Here the routing protocols attacks are analyzed.

A. TinyOS beaconing

TinySec is a light weight, generic security package that developers can easily integrate into sensor network applications. In TinyOS beaconing, any node can claim to be a base station. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject and alter transmitted data. Adversaries can interact with networks from a distance by inexpensive radio transceivers and power workstation. Resource consumption attacks, adversaries can repeatedly send packets to drain nodes battery and waste network bandwidth can steal node. It constructs a 'Breadth first' spanning tree rooted at the base station. Base station periodically broadcast route updates. The algorithm continues recursively with each node marking its parent as first node from which it hears a routing update during the current time epoch [3].All packets received or generated by a node are forwarded to its parents.

Attack: TinyOS beaconing protocol is highly susceptible to attack. Since routing updates are not authenticated, it is possible for any node to claim to be base station and become the destination of all traffic in the network. If routing updates are authenticated, laptop attacker can also use a HELLO flood attack to the whole network. Authenticated routing updates will prevent this attack.

B.Flat routing

Flooding is a technique used in sensor network. In flooding each node receive a data and then sent them to the neighbors by broadcasting till the destination of the packet is reached. It has several problems such as implosion, overlap and resource blindness. Gossiping protocol, nodes do not use broadcast but send the incoming packets to a randomly selected neighbor node. It can avoid implosion but cost effective [17].

C.Data centric

Perrig et al [7] has proposed SPIN belongs to secure routing protocols. SPIN: Sensor protocol for information via negotiation is among the early work to pursue a data-centric routing mechanism. Here a shared key is preinstalled at both the nodes and base station. It also uses TELSA for authentication. It is not suitable where the topology of the network changes frequently.

D.Directed Diffusion

This is data-centric routing protocol [12]. This algorithm aims at diffusing data through sensor nodes by using a naming scheme for the data. This can achieve energy saving but it has problems that is time synchronization techniques, which is not easy to realize and this lead to increase in the cost of sensor node. The various attacks due to robust nature of flooding are suppression, Cloning, replay of interest by the adversary, Selective forwarding and data tampering.

E.Geographic routing

Based on geographic routing, Tanochaiwiwan [13] develops a trusted routing protocol for location aware sensor networks called TRANS. In TRANS, the sensor node only sends data to neighbors with high trust value which often abandon the packets will be isolated, so the attacks of selective forwarding could be avoided. However, TRANS needs that each node knows its exact location information and its neighbors. This is energy expensive and unacceptable in some cases. All the protocols mentioned above are based on static key. GEAR [10] Geographic aware and Energy aware routing and GPSR [8] Greedy perimeter stateless routing, leverage nodes positions and explicit geographic packet destinations to efficiently disseminate queries and route replies. One drawback of GPSR is that packets along a single flow will always use the same nodes for the routing of each packet leading to uneven energy consumption. GEAR attempts to remedy this problem by weighting the choice of next hop by both remaining energy and distance from the target. The attack on this protocol is Sybil attack and location information can be misrepresented.

F.Cluster based protocols:

LEACH*:* Low-Energy Adaptive Clustering Hierarchy (LEACH) is one of the most popular hierarchical routing algorithms for sensor networks. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to sink. This will save energy since the transmissions will only be done by such cluster heads rather than all sensor nodes. LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it is not applicable to networks deployed in large regions. Furthermore, the idea of dynamic clustering brings extra overhead, which may diminish the gain in energy consumption. Deng et al [14] gives an intrusion toleration protocol INSENS, which represents Intrusion Tolerance Routing in WSN. It has two phrase which is route discovering and data transmission phrase. It uses symmetric key algorithm and can prevent intrusion. But here unchangeable key and the unidirectional function can be obtained by deception at ease, which leads the attack of false route and selective forwarding. Power Efficient Gathering Sensor Information Systems (PEGASIS) [11], sensors form a chain before perform sensing tasks. Each sensor finds the nearest sensor, which does not belong to the chain, and connects it to the chain. This procedure is repeated until there is no sensor that does not belong to the chain. The chain construction is performed in a greedy way. PEGASIS outperforms LEACH by eliminating the overhead of dynamic cluster formation and minimizes the number of transmissions and reception by using data aggregation. PEGASIS also introduces excessive delay for distant node on the chain. Threshold sensitive Energy Efficient sensor network protocol (TEEN) [5] is a hierarchical protocol deigned to be responsive to sudden changes in the sensed attributes**.** The idea is to form clusters and this process goes on the second level until sink is reached. TEEN is not good for applications where periodic reports are needed since the user may not get any data at all if thresholds are not reached.

Received: 20/02/2018. Published: 22/03/2018

Protocols	Attacks	Defenses
Tiny OS Beaconing	Selective Forwarding, Sink holes, Sybil attacks, Wormholes, HELLO Floods.	Secret shared key, link layer encryption, Unique symmetric key, Bi-directionality
Directed Diffusion	Selective forwarding, Sink holes, Sybil attacks, Wormholes, HELLO Floods.	Multipath routing, Braided paths, Unique symmetric key, Restricting the number of nodes by the base station.
Geographic routing (GPSR, GEAR)	Sinkholes, Wormholes	Use fixed topology like square, triangular or Hex Grid structure.
Cluster based protocols	Selective Forwarding, HELLO Floods.	Multipath routing, Braided paths, Bi-directionality.

G. Location based Protoco Most of the routing protocols for sensor networks require location information for sensor nodes. In most cases location information is needed to calculate the distance.

Conclusion

Today sensor network is one of the most important kinds of networks with many applications in the real life. Secure routing is critical for many sensor networks. Although many of these routing techniques look promising, there are still many challenges that need to be solved. In this paper, we summarize typical routing attacks on sensor networks and possible solutions against different attacks have also been outlined.

References

[1] Akyildiz, I.F., Sankarasubramaniam, Y., Cayirci, E.: “A survey on sensor networks”.IEEE communications Magazine, Vol. 40, (2002) 102-114.

[2] J.R.Douceur.,”The Sybil attack”. In first International workshop on peer-to-peer systems (IPTPS’02), Mar.2002.

[3]C.Karlof and D.Wagner,”Secure routing in wireless sensor networks: Attacks and Countermeasures”. In First IEEE International Workshop on Sensor Network protocols and Applications, Pages 113-127, May 2003.

[4]Xiajiang Do, Hsiao-Hwachen.,"Security in wireless sensor networks". Proc.IEEE wireless communicatios, August 2008.

[5]Zhong Su, Chung Lin, Feng Yuan Ren, Xiaosu Zhan, "Security mechanisms analysis of wireless sensor networks",Proc.fist international symposium on pervasive computing and applications, August 2006.

[6]James Newsome, Elane Shi, Dawn Song, Adrian Perrig, "The Sybil attack in sensor network: Analysis and Defenses", Proc.IPSN '04, April 2004.

[7]A.Perrig, R.Szewczyk, D.culler and J.Tygar, "Spins: Security Protocols for sensor networks", Proc. Mobile networking and computoing, 2001.

[8] Wuhao, Cheng Chao, Li Cheng,"Research on one kind of Improved GPSR secure routing protocol", Proc.International Symposium on microwave, Antenna, Propagation, and EMC Technologies for wireless communication, 2007.

[9]A. Manjeshwar and D. P. Agrawal, "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks", 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, 2001.

[10] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks,"UCLA Computer Science Department, Univ. Calif., Los Angeles, Tech.Rep.UCLA-CSD TR-01-0023, May 2001.

[11] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference, 2002

[12] Intanagonwiwat, C., Govindan, R. & Estrin, D.: "Directed diffusion for wireless sensor networks".IEEE/ACM Transactions Networking, Vol.11, (2003) 2-16. Constrain sensor networks".IEEE workshop on energy efficient wireless communication and networks, 2004.

[13]S.Tanochaiwiwan, P.Dave, R.Rhindwafe, "Location–Centric trust routing in Energy-Constrain sensor networks".IEEE workshop on energy efficient wireless communication and networks, 2004.

[14] J.Deng.R Han, and S.Mishra, "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks", The 23rd IEEE International conference on Distributed computing systems, 2003.

[15] Daniel Dallas, Chistropher,"Hop-count monitoring: Detecting sinkhole attacks in WSN", Proc IEEE 2007.

[16]Ishizuka, M.Aida,"Performance study of node placement in sensor network "In distributed computing systems workshop, 2004.Proc.24th International Conference on 23-24 March 2004.pages 593-603.

[17]Shijin Dai, Lemin Li,"Research and analysis on routing protocols for WSN".IEEE 2005.

[18]Liu Yu, Wang Yu-mei,"Sensor Deployment in Energy Efficient Wireless Sensor Networks", Proc.IEEE 2005.

[19]Bo Yu, Bin Xiao,"Detecting Selective Forwarding Attacks in Wireless sensor networks", Proc.IEEE 2006.

[20]Yu and Xiao,"Detecting selective forwarding attacks in wireless sensor networks," Proc IEEE ISPDP 2006.

[21]H.M sun, Hsu, Chen"Mobile jamming attack and its countermeasure in wireless sensor networks," IEEE 2007.