KIET IJCE

KIET International Journal of Communications & Electronics
Volume. No. 1, Issue No. 1, Mar – Jun 2013, ISSN: 2320 - 8996

# A Survey on Issues, Attacks and Countermeasures on the Network Layer in Wireless Sensor Networks

[1]Sunil Kumar,[2]C. Rama Krishna, [3],A. K. Solanki
[1]Research Scholar, Punjab Technical University, Jalandhar (Punjab), India.
[2]NITTTR/Computer Science & Engineering, Chandigarh (Punjab), India.
[3]BIET /Computer Science & Engineering, Jhansi (U.P), India.
[1]sunilymca2k5@gmail.com,[2]rkc_97@yahoo.com,[3]solanki_biet07@hotmail.com

***Abstract*- Due to the intrinsic nature of the network and application scenario, Wireless Sensor Networks (WSNs) are vulnerable to many attacks. In this paper, we describe briefly issues related to network layer and different attacks such as Sybil, sinkhole, wormhole, hello flood, selective forwarding, neglect and greed, homing, misdirection and black hole attacks and their countermeasures. Also, this paper discusses known approaches of security detection and defensive mechanisms against the network layer attacks; this would enable it security managers to manage the network layer attacks of WSNs more effectively. Protecting WSNs against different attacks - while remaining low-cost and flexible - is a primary research challenge that bears further exploration.**

***Keywords:*** **Sensor networks, issues, attacks, countermeasures.**

## I. INTRODUCTION

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

The paper is organized as follows: Section-I provides a brief overview of wireless sensor networks. Section-II describes different types of Issues at the network layer in WSNs. Section-III describe various security attacks and their countermeasures against Security attacks. Section-IV concludes the paper for future directions.

## II. ISSUES AT THE NETWORK LAYER

Sensor networks are being built for specific purposes. Routing is most important part of WSN for sending the data from sensor nodes to base station. At the network layer various issues are [1, 2, 3, 4]:

1. Energy efficiency is a very important issue at the network layer. There is a need to discover different techniques to eliminate energy inefficiencies that may shorten the lifetime of the network. There is a need to find various methods for discovering energy efficient routes and for relaying the data from the sensor nodes to the base station at the network layer to optimize the lifetime of a wireless sensor.
2. Multi- path design technique should be incorporated in the routing protocols. Multi-path technique is applied in those protocols which set up multiple paths so that a path among them can be used when the primary path is failed.
3. The repairing of path is desired in routing protocols whenever a path break is detected. Routing protocols should be able to find a new path at the network layer even if some nodes fail or blocked due to some environmental interference.
4. In the network layer in order to maximize energy savings there is a need to provide a flexible platform for performing routing and data management.
5. The data traffic that is generated will have significant redundancy among individual sensor nodes. The routing protocol should exploit such redundancy to improve energy and bandwidth utilization.
6. There is need to develop a routing protocol that have the property of multiple wireless hops as the nodes are scattered randomly resulting in an ad hoc routing infrastructure.
7. Routing Protocols should be like that they can take care of homogeneous as well as heterogeneous nature of the nodes i.e. each node will be different in terms of computation, communication, operating system (TinyOS, ZigBee etc.) and power.

Various types of routing protocols for WSNs are: Sensor Protocols for Information via Negotiation (SPIN), Rumor Routing, Direct Diffusion, Low Energy Adaptive Cluster Hierarchy (LEACH), Power Efficient Gathering in Sensor Information System (PEGASIS), Threshold sensitive Energy Efficient sensor Network protocol (TEEN), Geographic and

Energy Aware Routing (GEAR), Sequential Assignment Routing (SAR), Hybrid Energy Efficiency Protocol (HEEP) and others.

## II. SECURITY ATTACKS AND THEIR COUNTERMEASURES

### 1. Sybil Attacks

In a *Sybil attack*, an attacker presents multiple identities [5]. Coupled with insecure location claims, this means an attacker can appear to be in multiple places at the same time. By creating fake identities of nodes located at the edge of communication range all around a victim, chances are high that the attacker will be chosen as the next-hop in geographic forwarding. The attack can also degrade any guarantees made by a multipath routing scheme, making selective forwarding easy.

**Countermeasures**

Identity fraud is central to the Sybil attack; hence proper *authentication* is a key defense [6]. A trusted key server or base station may be used to authenticate nodes to each other and bootstrap a shared session key for encrypted communications, as in SPINS [7]. This requires that every node share a secret key with the key server. If a single network key is used, compromise of any node in the WSN would defeat all authentications. Another countermeasure is *location verification*. Sastry et al. describe a simple protocol that uses the difference in time-of-flight of radio and sound waves to securely verify location claims [8]. The combination of these two countermeasures, verifying identities and locations, would prevent Sybil-based DOS attacks.

### 2. Sinkholes Attacks

In *sinkhole* attacks [6] an attempt is made to lure traffic from the sensor network to pass through an adversary. Low-cost routes may be erroneously flooded to lure the traffic, or a wormhole attack could be mounted to actually provide a low-cost route. In either case, the objective for the attacker is to be positioned such that other selective forwarding attacks, or merely eavesdropping, are easier to do.

**Countermeasures**

One approach to avoiding sinkholes attacks is to use routing algorithms that are *resistant* to arbitrary configurations, such as geographic forwarding [9, 6]. Since each node makes an independent forwarding decision based on the location of its neighbors, it is not as easy to attract routing to an attacker. Communicating parties may also use *end-to-end verification* of advertised latency or quality to detect when a path may contain an unwarranted diversion [6]. Upon detecting a problem, nodes may attempt *systematic rerouting* to avoid the malicious node [10].

### 3. Wormholes Attacks

In a *wormhole* attack, adversaries cooperate to provide a low-latency side-channel for communication [11]. For example, two attackers may possess a second radio for communicating over a higher-power, long-range link. Messages received at one attacker are relayed to the other using the side-channel, where they are transmitted as if only one-hop away from the original source. This ability to understate ones distance from another node may cause neighboring nodes to favor the attacker for routing is another example of a sinkhole. As long as the side-channel exists, service may actually be enhanced, instead of denied. However, when the attacker moves or ceases to tunnel messages, the network may be left in an inconsistent state that requires re-initialization of some services to restore proper function.

**Countermeasures**

As described for sinkholes attacks, *geographic forwarding* is a tamper-resistant routing protocol. Each message is forwarded individually, choosing the next-hop node to be the neighbor closest to the ultimate destination. Such a scheme would not favor a wormhole in the network, though it may coincidentally use it. Hu et al. describe a defense based on *packet leashes*, where the distance that a message may travel in a single hop is limited [11]. Each message includes a timestamp and the location of the sender. The receiver compares these with its own location and time to determine if the maximum transmission range has been exceeded. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs.

### 4. HELLO Floods Attacks

*HELLO flood* is a single broadcast by a powerful adversary to many members of the WSN, announcing false neighbor status [6]. Many protocols use the exchange of HELLO messages to establish local neighborhood tables. The result of a HELLO flood is that every node thinks the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Retransmission attempts to the absent attacker cause traffic congestion and confusion in the entire routing system.

**Countermeasures**

Verifying the *bi-directionality* of local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices [6]. However, if the attacker can use a sensitive receiver, it can eventually convince nodes in the network of its legitimacy. *Authentication*, as described for the Sybil defense, is also a possible solution. Nodes can use a trusted third-party to verify the authenticity of each of its neighbors before forwarding messages to them.

### 5. Selective Forwarding Attacks

WSNs usually depend on every node to take part in routing for its neighbors if it can provide a desirable forwarding path. Various *selective forwarding* attacks can exploit this dependence to cause DOS via routing. A subverted sensor device can simply *neglect* to forward certain messages. A random dropping policy raises the local loss rates and may

induce costly end-to-end recovery mechanisms. An attacker may also drop messages to or from certain victims, such as base stations or other servers. At an extreme, a node could not only refuse to forward any packets, but could advertise a desirable path to its neighbors, creating a routing *blackhole*. Any messages passing nearby will be diverted to the adversary, where they are silently dropped. In addition to causing a DOS to the senders of the messages, neighbors of the adversary suffer from increased contention due to the above-normal levels of traffic.

**Countermeasures**

Using *multiple disjoint routing* paths [12] and *diversity coding* [13] can mitigate the effect of the attack. These countermeasures lessen the probability that a message will encounter an adversary along all routes to the destination. Diversity coding sends encoded messages along multiple paths, such that the originals can be reconstructed to conceal message loss, without the cost of full duplication. To counter these defenses, an attacker must subvert additional nodes along the disjoint paths or choose an important source to move closer to, where jamming will be effective. Nodes can also *monitor* their neighbors to gain probabilistic assurance that messages are being correctly forwarded. A node relays a message to its neighbor and then listens to the wireless channel, noting whether it overhears the neighbor's subsequent broadcast [14] of the same message. Although collisions, collusion, and asymmetric communication links limit the sender's ability to monitor every packet, the forwarding ratio can be used to inform a quality-rating mechanism. This mechanism is responsible for choosing a next-hop neighbor that has a high probability of properly forwarding subsequent messages. Periodic end-to-end *probing* [15] can also alert a node to troublesome network paths, whether from congestion or malicious neglect. If an adversary can distinguish the probes from normal traffic, however, he can properly forward them so as not to arouse suspicion.

### 6. Neglect and Greed Attacks

If a node drops packets or denies transmitting legitimate packets or if a node is very greedy to give undue priority to its own messages, these could be considered as '*neglect and greed*'. Dynamic Source Routing (DSR) protocol or the protocols that are based on DSR are especially vulnerable to this type of attack.

**Countermeasures**

Use of multipath routing or redundant message transmission could be the solutions for handling neglect and greed attacks. However, for WSNs these solutions might not be feasible. Instead, use of some other routing mechanisms could be helpful.

### 7. Homing Attacks

Sometimes in WSNs, some nodes are given some special responsibilities like managing cryptographic keys, making use of acquired data, maintaining a local group, etc. Often the adversaries are attracted to these leader nodes and try to eavesdrop on their activities. In case of *homing attack*, the adversaries try to hamper the normal functioning of such types of leader nodes within a WSNs. Homing attack is especially dangerous for the location-aware routing protocols which rely on geographic information.

**Countermeasures**

Different types of cryptographic schemes, algorithms, hiding management messages, etc. could be used for preventing homing attacks.

### 8. Misdirection Attacks

By forwarding messages along wrong paths, an attacker *misdirects* them, perhaps by advertising false routing updates. An attacker could DOS a particular sender by diverting only traffic originating from the victim node. A receiver could likewise be denied service if the attacker diverts traffic away from the node. This may be possible by rewriting the downstream path in routing algorithms which embed source-routes in each packet. An attacker can also forge a source address when sending a request, so that the response will return to the victim. This could be done to confuse the victim or to flood it, if a service provides a mechanism for traffic amplification.

**Countermeasures**

Routing updates should be *authenticated* to prevent malicious modification by untrusted adversaries [16]. A freshness mechanism can protect against replay attacks, while cryptographic integrity checks protect against unauthorized modification of a message while in transit. In WSNs that use a hierarchical structure for routing, *egress filtering* may be appropriate. Nodes which serve as collection points for subordinates' traffic may examine each message before forwarding it. Messages with source addresses that could not legitimately originate at lower levels of the hierarchy are discarded.

### 9. Black Hole Attacks

The black hole attack is one of the simplest routing attacks in WSNs. In a black hole attack, the attacker receives all the messages but does not forward all the messages he receives, just as a black hole absorbing everything passing by. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it, is dramatically decreased. Different locations of the attacker induce different influences on the network. If the attacker is located close to the base station, all the traffic going to the base station might need to go through the attacker. Obviously, black hole attacks in this case can break the communication between the base station and the rest of the WSNs, and effectively prevent the WSNs from serving its purposes. In contrast, if a black hole attacking node is at the edge of the WSNs, probably very few sensors need it to communicate with others. Therefore, the harm can be very limited.

**Countermeasures**

Black hole attack which modifies routing messages can be provoked by the use of source authentication. Digital signature, message authentication code (MAC), hashed MAC (HMAC) can be used. Up to certain level of security can be attained at network layer in internet by the use of IPSec. Authenticated Routing for Ad-Hoc Networks (ARAN) is another routing protocol which provides the protection from Black Hole attack where there is threat to the changes in sequence number, hop count modification, source routing changes and spoofing of destination addresses [17].

## IV. CONCLUSION & FUTURE WORK

The survey on wireless sensor network security is vast with various attack models and counter measures proposed by various researchers. Various methodologies are presented for ensuring security at the network layer in WSNs has been surveyed. We have discussed different issues and attacks that spoil the functioning of the network layer. We have also covered the countermeasures and potential solutions against those network layer attacks. Hopefully by reading the survey, the readers can have a better view on issues, attacks and their countermeasures at network layer in WSNs.

Sensor networks are still at an early stage in terms of technology as it is still not widely deployed in real world and this opens many doors for research. The standard models of current attacks and countermeasures are able to help increase security developers' understanding and pave the way for building more secure WSNs. In the future, we will analyze network layer attacks using various UML diagrams - an activity diagram, state diagram, class diagram, composite structure diagram, and interaction diagram - to analyze the current attacks and countermeasures in a sophisticated way.

## REFERENCES

[1]. Limin Wang, "Survey on Sensor Networks", Department of Computer Science & Engineering, Michigan State University, 2004.

[2]. K. Akkaya and M. Younis, "A survey of Routing Protocols in Wireless Sensor Networks", Elsevier Ad Hoc Network Journal, 2005, pp. 325-349.

[3]. Deepak Ganesan et.al, "Networking Issues in Wireless Sensor Networks", Elsevier Science, 9th December, 2005.

[4]. P. Jiang, Yu Wen et.al,"A Study of Routing Protocols in Wireless Sensor Networks", In Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21-23, 2006, Dalian, China.

[5]. John R. Douceur, "The Sybil attack" In IPTPS, pages 251-260, 2002.

[6]. Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *In First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[7]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks", *In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001*, pages 189-199, July 2001.

[8]. Naveen Sastry, Umesh Shankar, and David Wagner. "Secure verification of location claims", *In ACM Workshop on Wireless Security (WiSe 2003), September 2003*.

[9]. G. G. Finn, "Routing and addressing problems in large metropolitan-scale internetworks", Technical Report ISI/RR-87-180, ISI, March 1987.

[10]. Jessica Staddon, Dirk Balfanz, and Glenn Durfee "Efficient tracing of failed nodes in sensor networks", *In Proceedings of the first ACM international workshop on Wireless sensor networks and applications* (WSNA), pages 122-130. ACM Press, 2002.

[11]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson "Packet leashes: A defense against wormhole attacks in wireless networks", *In Proceedings of IEEE Infocom 2003*, April 2003.

[12]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", *Mobile Computing and Communications Review*, 4(5), October 2001.

[13]. E. Ayanoglu, I. Chih-Lin, R. D. Gitlin, and J. E. Mazo, "Diversity coding for self-healing and fault tolerant communication networks", *IEEE Trans. Comm*., COM-41:1677-1686, November 1993.

[14]. Sergio Marti, Thomas Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM-00), pages* 255-265, N. Y., August 2000.

[15]. Steven Cheung and Karl Levitt, "Protecting routing infrastructures from denial of service using cooperative intrusion detection", *In New Security Paradigms Workshop, Cumbria*, UK, September 1997.

[16]. Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks. *IEEE Network*, 13(6):24.30, 1999.

[17]. H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless Ad-Hoc networks," Cincinnati Univ.,OH, USA; *IEEE Communications Magazine, , Vol.40*, pp.70- 75, ISSN: 0163-6804, Oct. 2002.

[18]. Tian Bin, Ouyang Xi, Li Dong, Luo Shoushan, Yang Yixian, Xin Yang, "Study of Attacks and Countermeasures in Wireless Sensor Networks", *Advances in information Sciences and Service Sciences(AISS) Volume 4, Number 8*, May 2012. Vol. l4 pp.-311-320.

[19]. Modares H., R. Salleh and A. Moravejo sharieh, "Overview of Security Issues in Wireless Sensor Networks", *Computational Intelligence, Modelling and Simulation (CIMSiM), Third International Conference on*, pp. 308-311, 2011.

[20]. D.G. Anand, H.G. Chandrakanth, M.N. Giriprasad, "Security Threats & issues in wireless sensor networks", *in International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1*, Jan-Feb 2012, pp. 911-916.

[21]. Mohammad Sadeghi, Farshad Khosravi, Kayvan Atefi, Mehdi Barati, "Security Analysis of Routing Protocols in Wireless Sensor Networks", *(IJCSI) International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3*, January 2012, pp. 465-472.

[22]. Muhammad R Ahmed, Xu Huang, and Dharmendra Sharma, "A Taxonomy of Internal Attacks in Wireless Sensor Network" *World Academy of Science, Engineering and Technology*, 2012, pp. 427-430.