ISSN 2319 - 6629
Volume 5, No.3, April – May 2016
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt01532016.pdf

A Survey On Comparison Of Secure Routing Protocols in Wireless Sensor Networks

Shipra Suman[1], Shubhangi[2]
[1]SHIATS,Allahabad, India, shipra.suman92@gmail.com
[2] SHIATS, Allahabad, India, shubhangivaish4@gmail.com

ABSTRACT

Wireless Sensor Network (WSN) at the present time is a major growing technology. Sensor networks provide a powerful combination of distributed sensing, computing and communication. They lend themselves to countless applications including security and surveillance, control, actuation and maintenance of complex systems but at the same time offer numerous challenges due to their peculiarities.WSN face security attacks already experienced by Internet and wireless ad hoc networks. In this paper, we present the attacks on WSN and compare some secure routing protocols of sensor networks.

Keywords—Blackhole attack, Sybil attack, SPIN, LEACH, TARF, SIGF, LEAP, WSN, Wormhole attack.

1. INTRODUCTION

Wireless Sensor Network(WSN) is a collection of sensing devices that can communicate wirelessly. Each device can sense, process and talk to its peers[4]. Basically, sensor networks are application dependent. Sensor networks are primarily designed for real-time collection and analysis of low level data in hostile environments. For this reason they are well suited to a substantial amount of monitoring and surveillance applications. Popular wireless sensor network applications include wildlife monitoring, bushfire response, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates etc[1]. To collect data from WSNs, base stations and aggregation points are commonly used. They usually have more resources (e.g. computation power and energy)than normal sensor nodes which have more or less such constraints. Aggregation points gather data from nearby sensors, integrate the data and forward them to base stations, where the data are further processed or forwarded to a processing centre. In this way, energy can be conserved in WSNs and network life time is thus prolonged[2].

Majority of the sensor networks are deployed in hostile environments with active intelligent opposition. Hence security is a crucial issue. One obvious example is battlefield applications where there is a pressing need for secrecy of location and resistance to subversion and destruction of the network. Less obvious but just as important security dependent applications include disasters especially those induced by terrorist activities, it may be necessary to protect the location of casualties from
unauthorized disclosure, or in applications where chemical, biological or other environmental threats are monitored, it is vital that the availability of the network is never threatened. Attacks causing false alarms may lead to panic responses or even worse total disregard for the signals[1].

WSN uses a wireless channel to communicate, so there are inevitably some issues such as message interception, tampering and other security issues. Therefore, the security of networks has an important impact on the performance of monitoring, system availability, accuracy, and scalability, etc[3]. In this paper, we have compared some of the security routing protocols and have elaborated the attacks happening on them.

2. SECURITY GOALS IN WSN

We can classify the security goals into two goals: main and secondary. The main goals include security objectives that should be available in any system (confidentiality, availability, integrity and authentication). The other category includes secondary goals (self -organization, secure localization, Time synchronization and Resilience to attacks) [5] [6]. Figure 1 shows the classification of security goals in WSN.

- **Confidentiality** (Forbid access to unwanted third parties).
- **Authentication** (Identity verification and validation).
- **Availability** (Service has to be always available).
- **Integrity** (Data is exchanged without malicious alteration).
- **Self Organization**(Every sensor node needs to be independent and flexible enough to be self-organizing and self-healing).
- **Secure localization** (Sensor network often needs location information accurately and automatically).
- **Time synchronization** (Sensor radio may be turned off periodically in order to conserve power).

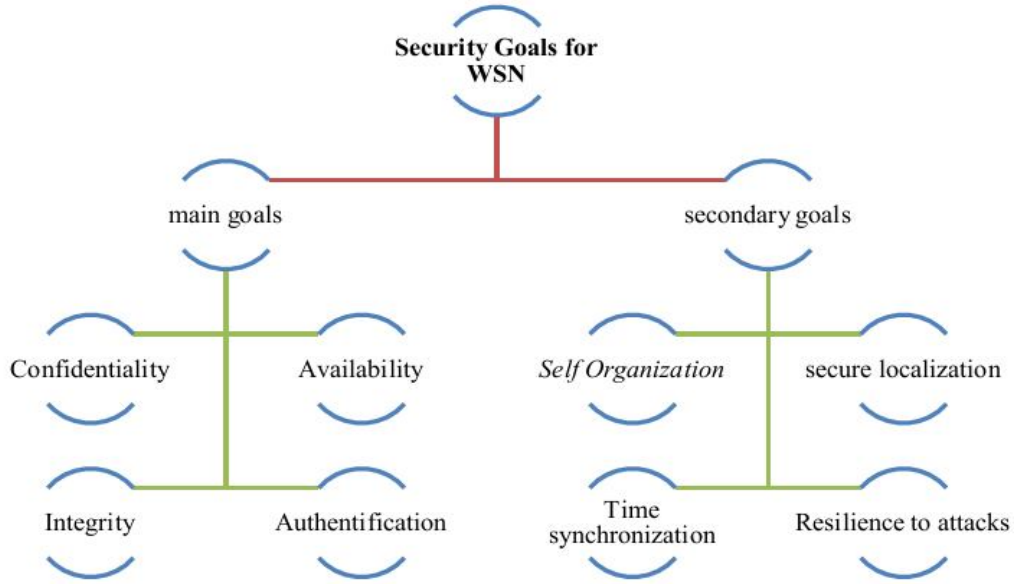

Figure 1.Security goals of WSN

- **Resilience to attacks** (The covenant of a single node must not violate the security of the whole network).

3. SECURITY ATTACKS IN WSN

The different characteristics of wireless sensor networks (energy limited, low-power computing, use of radio waves, etc.) expose them to many security threats. We can classify the attacks into two main categories [7]: Active and Passive. In passive attacks, attackers are typically camouflaged, i.e. hidden, and tap the communication lines to collect data. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Several papers have presented the security attacks in WSN [8][10][11][12].

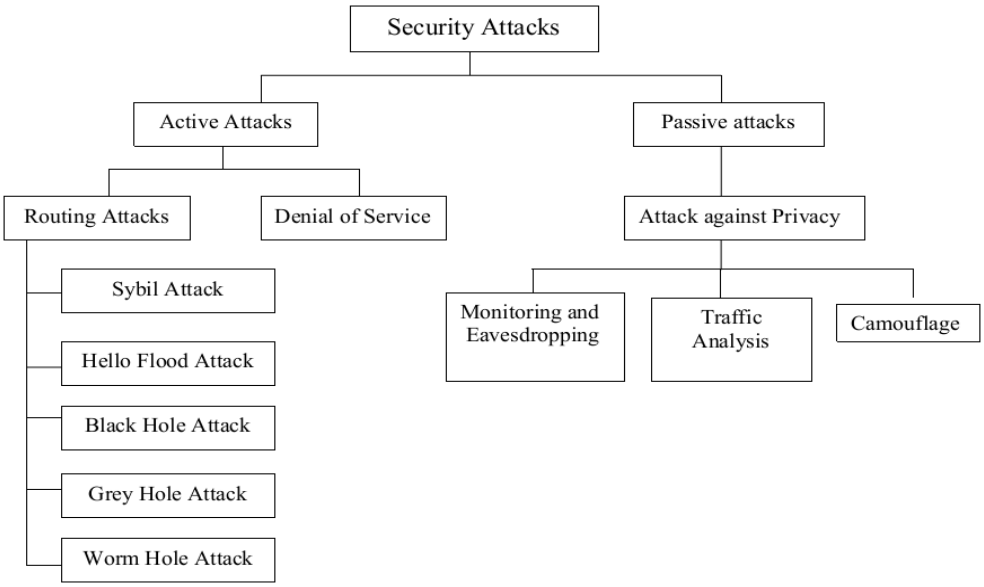

Figure 2.Classification of attacks on WSNs

Figure 2 classifies the different types of security attacks in WSN. These attacks are discussed as follows :

- *Spoofed, altered or replayed routing information***:** May be used for loop construction, attracting or repelling traffic, extend or shorten source route.

- *Selective forwarding***:** In this attack, the attacker prevents the transmission of some packets. They will be removed later by the malicious node.

- *Wormhole attack***:** The wormhole attack requires insertion of at least two malicious nodes. These two nodes are interconnected by a powerful connection for example a wired link. The malicious node receives packets in one section of the network and sends them to another section of the network. Figure 3 illustrates the wormhole attack.

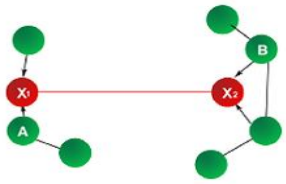

Figure 3. Wormhole attack

- *Sybil attack:* The Sybil attack is shown by figure 4. A malicious node presents multiple identities to the other nodes in the network. This poses a significant threat to routing protocols and will cause the saturation of the routing tables of the nodes with incorrect information.

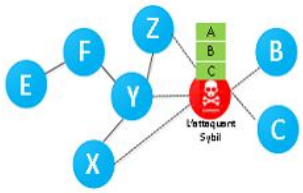

Figure 4. Sybil attack

- *Eavesdropping and passive monitoring:* This is the most common and the easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, eavesdropping on these messages prove more effective for an adversary.

- *Black hole attack:* The attack involves inserting a malicious node in the network. This node, by various means, will modify the routing tables to force the maximum neighboring nodes passing the information through it. Then like black hole in space, all the information that will go in it will never be retransmitted. Figure 5 depicts the black hole attack.

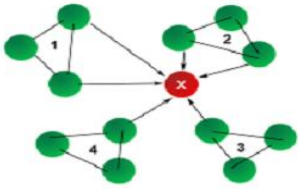

Figure 5. Black hole attack

- *Hello Flooding Attack*: Discovery protocols on WSNs use HELLO messages types to discover its neighboring nodes. The hello flooding attack is shown by figure 6. In an attack type HELLO flooding, an attacker will use this mechanism to saturate the network and consume energy.

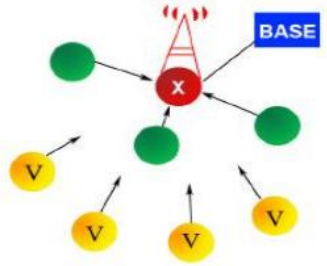

Figure 6. Hello flooding attack

- *Routing table overflow:* In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized node present in the network. The main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes. Proactive routing protocols are more vulnerable to this attack compared to reactive routing protocols.

- *Routing table poisoning:* In this case, the compromised nodes in the network send fictitious routing updates or modify genuine route update packets sent to other honest nodes. Routing table poisoning may result in sub-optimal routing, congestion in some portions of the network, or even make some parts of the network inaccessible.

- *Node replication***:** In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power and other resources available to the nodes and also causes unnecessary confusion in the routing process.

4. SECURE ROUTING PROTOCOLS IN WSN

The goal of a secure routing protocol for a WSN is to ensure the integrity, availability of messages and authentication. Most of the existing secure routing algorithms for WSNs are all based on symmetric key cryptography except the work in (Du et al., 2005), which is based on public key cryptography. In the following sub-sections, some of the existing secure routing protocols for WSNs are discussed in detail.

- *SPIN:* Sensor Protocols for Information via Negotiation (SPIN) that disseminates all the information at each node to every node in the network assuming that all nodes in the network are potential BSs. The SPIN family of protocols uses data negotiation and resource -adaptive algorithms. Nodes running SPIN assign a high-level name to completely describe their collected data (called meta -data) and perform metadata negotiations before any data is transmitted. In addition, SPIN has access to the current energy level of the node and adapts the protocol it is running based on how much energy is remaining. The SPIN family is designed to address the deficiencies of classic flooding by negotiation and resource adaptation [12].

- *LEACH:* Low Energy Adaptive Clustering Hierarchy. These protocols uses cluster node for the purpose of transmission of information between the nodes. It is a self-organizing protocol and nodes organize themselves into local clusters and perform data transmission to the Selection of cluster head node is not fixed and it depends on possibility of nodes, which possess high energy. Formation of cluster head is based on TDMA schedule for data transmission. Time Division Multiple Access(TDMA) used as a scheduling mechanism makes it prone to long delays when applied to large sensor networks. TDMA schedule prevents data collision, among messages and preserve energy among non cluster nodes [13]. Figure 7 shows the clustering in LEACH protocol.

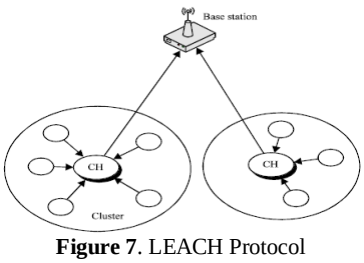

Figure 7. LEACH Protocol

- *SIGF:* SIGF (Secure Implicit Geographic Forwarding), a configurable secure routing protocol family for wireless sensor networks that provides "good enough" security and high performance. By avoiding or limiting shared state, the protocols pre-vent many common attacks against routing, and contain others to the local neighborhood. SIGF makes explicit the tradeoff between security provided and state which must be stored and maintained. It comprises three protocols, each forming a basis for the next: SIGF-0 keeps no state, but pro-vides probabilistic defenses; SIGF-1 uses local history and reputation to avoid attackers; and SIGF-2 uses neighborhood-shared state to provide stronger security guarantees [14].

- *TARF:* To fight against the "identity theft" threat arising from packet replaying, trust management is introduced into WSNs, proposing TARF - a Trust-Aware Routing Framework for wireless sensor networks[15]. TARF identifies those malicious nodes that misuse "stolen" identities to misdirect packets by their low trustworthiness, thus helping nodes circumvent those attackers in their routing paths. TARF secures the multi-hop routing in WSNs against intruders exploiting the replay of routing information by evaluating the trustworthiness of neighboring nodes. TARF is also energy-efficient, highly scalable, and well adaptable.

- *LEAP:* LEAP (Localized Encryption and Authentication Protocol), a key management protocol for sensor net-works that is designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node [16]. LEAP is very effective in defending against many sophisticated attacks such as HELLO Flood attack, Sybil attack, and Wormhole attack. Karloff and Wagner [17] have studied various attacks on the security of routing protocols for wireless sensor network. In LEAP routing control information is authenticated by local broadcast authentication scheme, which prevents most outsider attacks.

Table 1 shows the comparison of secure routing protocols with respect to the attacks in Wireless Sensor Network. From that it is found that all the discussed secure routing protocols are prone to the hello flood attack. Further it is found that the KeyChain protocol is only exposed to two attacks namely route poisoning attack and replay attack. Also the SPIN routing protocol is open to all the mentioned attacks whereas LEAP, SIGF, TARF and LEACH routing protocols are open to either one or two of the mentioned attacks.

PROTOCOLS→ ATTACKS↓	SPIN	LEAP	SIGF	TARF	LEACH	KeyChain
Eavesdropping	Yes	Yes	Yes	Yes	Yes	No
Route Poisoning	Yes	No	Yes	No	Yes	Yes
Blackhole	Yes	Yes	Yes	Yes	Yes	No
Grayhole	Yes	Yes	Yes	Yes	Yes	No
Wormhole	Yes	No	No	Yes	Yes	No
Replay	Yes	Yes	Yes	No	Yes	Yes
Sybil Attack	Yes	Yes	Yes	Yes	Yes	No
Hello Flood	Yes	Yes	Yes	Yes	Yes	Yes
Node Replication	Yes	Yes	No	No	No	No

Table 1. Comparison of secure routing protocols with respect to attacks in WSN.

5. CONCLUSION

In this survey, firstly we have given the security goals of a network. Next we have classified the attacks in WSN in two categories i.e. active and passive attacks. Further, we have given the definition of these types of attacks. Thus, it can be concluded that wireless sensor networks are very exposed to the attacks as the nodes are unguarded in a hostile and dangerous environment. Hence, a system is required for its security as the discussed routing protocols are not fully secure. We have presented in this paper with different types of attacks, secure routing protocols that defend these attacks. We have also presented with a tabular classification of these protocols against the attacks in the hope that this will help the researchers to come up with smarter and more robust security. According to this classification, we infer that performance of Key Chain protocol is better amongst the others because it is prone to less number of attacks. We hope that this survey will help future researches in developing a good knowledge about the attacks and their countermeasures.

REFERENCES

1. Dr. G. Padmavathi, D. Shanmugapriya, "**A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks**", *International Journal of Computer Science and Information Security*, Vol. 4, No. 1 & 2, 2009.
2. Kai Xing, S S R Srinivasan, M Rivera, J Li , X Cheng, "**Attacks and Countermeasures in Sensor Networks: A Survey**", *Network security 2005 Springer.*
3. P Sharma, M Saluja and K K Saluja, "**A Review of Selective Forwarding attacks in Wireless Sensor Networks**", *International Journal Of Advanced Smart Sensor Network Systems* ,Vol 2,No.3, July 2012.
4. D Puccinelli, "**The Basics of Wireless Sensor Networking and its Applications**", *http://web.dti.supsi.ch/~puccinelli.*
5. Q I Sarhana, "**Security Attacks and Countermeasures for Wireless Sensor Networks: Survey**", *International Journal of Current Engineering and Technology*, June 2013.
6. Z. Benenson, M. Cholewinski, C. Freiling, "**Vulnerabilities and Attacks in Wireless Sensor Networks**", *Laboratory for Dependable Distributed Systems, University of Mannheim*, Germany, 2010.
7. E. Çayırcı and C. Rong , "**Security in Wireless Ad Hoc and Sensor Networks**", *John wiley and sons Ltd., ISBN: 978-0-470-02748-6*, 2009.
8. P. Mohanty, S. Panigrahi, N. Sarma and S. Satapathy, "**Security issues in wireless sensor network data gathering protocols: a survey**", *Department of Computer Science and Engineering Tezpur University, Tezpur, India* 2010.
9. A. Singla, R. Sachdeva, "**Review on Security Issues and Attacks in Wireless Sensor Networks**", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 4, April 2013.
10. V. Soni1, P. Modi, V. Chaudhri, "**Detecting Sinkhole Attack in Wireless Sensor Network**", *International Journal of Application or Innovation in Engineering & Management*, Volume 2, Issue 2, February 2013.
11. K. Sharma, M. Ghose, "**Wireless Sensor Networks: An Overview on its Security Threats**", *IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs*, 2010.
12. M. Bani Yassein, A al-zoubi, Y Khamayseh, W. Mardini ,"**Improvement on LEACH Protocol of Wireless Sensor Network (VLEACH)",** . *International Journal of Digital Content Technology and its Applications, 3(2), 182-18.*
13. Amir Sepasi Zahmati et. al, "**An Energy-Efficient Protocol with static Cluster based Routing in Wireless Sensor Networks**," *World Academy of Science, Engineering and Technology* 28 2007.
14. Brian Blum, Tian He, Sang Son, and John Stankovic. "**IGF: A state-free robust communication protocol for wireless sensor networks**", *Technical Report ,University of Virginia, Charlottesville, VA, 2003.*
15. R. Anderson, M. Kuhn. "**Tamper Resistance – A Cautionary Note",** *The Second USENIX Workshop on Electronic Commerce Proceedings*, November 1996.
16. C. Karlof and D. Wagner. "**Secure Routing in Sensor Networks: Attacks and Countermeasures**," *Proc. of First IEEE Workshop on Sensor Network Protocols and Applications*, May 2003.