THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

A Survey on Security of Routing Protocols and Their Performance For Wireless Sensor Network

Vipin Kumar
vipin.17730@lpu.co.in
School of Computer Science and Engineering
Lovely Professional University Punjab India

Abstract:

In a wireless sensor networks are widely used in many applications. To tracking the event and collecting the data from remote area or hostile area wireless sensor network is used. A WSN is the collection of wirelessly connected tiny sensors that has very limited resources like battery, computation power and memory. When data is collected by some sensor in must be transfer to control centre through gateway (Sink). Routing protocol route the date to the sink. Transfer the data to sink securely is very important task. For secure transfer of data in the network routing protocol must be secure and can be use the cryptography method for authentication and confidentiality. When some security technique applies to routing the performance of routing protocol may be degrading. In this paper we try to analyse the security of these routing protocol and their performance.

Key words: Routing, Security, Authentication, Network Layer and Performance.

1. Introduction:

Wireless Sensor Networks (WSNs) are collection of small sensors that sense the data from the physical world according to requirements such as temperature, pressure, humidity, speed, motion, etc.[1][2]. This information can be accessed through the door to the drain. Sensors are deployed in large numbers due to their wireless nature; they work easily in any environment. Many applications of tracking and monitoring of area is depend on sensors. Some typical applications include border security area monitoring, forest fire detection [3]. The security of such network is very important and there must be a robust security technique to protect these systems [4]. In this paper we try to summaries the different attack in WSN and what are the security mechanisms used for securing routing protocol to flowing the data properly in the network.

2. Attacks on WSN

A WSN is vulnerable of different types of attacks that may disturb the routing of data in the network. Spoofing attack changes the routing information and disturbs the routing of data.

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

There are other attack like selective forwarding in which a selfish node drop some of the packets and forwarding only selective packets [5]. A Sinkhole attack make a node as sink that not forward any packet and no information is flow in the network after this node [6]. A sybil attack in which a node present many identity. These type of node known as malicious node [7]. There are other types of attacks wormhole, blackhole and grayhole attack where malicious node advertise false path pretended as it is as good one. A hello flood attack in which attackers are busy with the network by sending a huge number of greeting messages so that node is not in the state to process any fruitful information. The attacker node eventually wrongly transmits a shorter route to the base station and all the nodes receiving the HELLO packets are attempting to transmit to the attacker node. Those nodes are out of the attacker's radio range, however.

3 Security requirements

Security requirements for WSN are the same as any other network that includes confidentiality of data and message and authentication communicating identity. Confidentiality is the hide of information that is only authorizing person can see the message or can have access the information. There is some information that required higher confidentiality such as military applications. To reveals the content of such data is the serious thread for a nation. In any communication authentication is very important as every user must ensure that he is communication with correct user and information is not going to the wrong hands. .If authentication of a user has not been done properly an unauthorized user may see the information and change the information. So security is very important in these types of networks.

4. Routing Challenges in WSN:

Wireless sensor network routing varies in different ways from traditional routing in fixed networks. There is no network, wireless connections are unreliable, sensor nodes can fail, and routing protocols must meet stringent requirements for energy saving [8]. For wireless networks in general, several routing algorithms have been developed. There are many routing protocols. In WSN there are tiny nodes that have very limited resources like battery power, computation speed, and storage. Strong encryption and decryption algorithms are not suitable for these tiny nodes. There the some lightweight techniques for encryption but these are very limited and take storage and battery of node. In this case node exhausted their battery and become dead. In this type of network communication is multi hope and data is transfer from

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

node to sink through many nodes. So in network node to node security is required and end to end security is also required. If some cryptography techniques apply in sensor network key management is also a big issue in these type of networks. There are many attacks on network of security of these network is required.

Table 1: Routing Protocols for WSNs

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocols	SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, Gradient-Based Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based protocols	SAR, SPEED, Energy-aware routing

5. Secure Routing Protocol

In 2003 Zhu and S. Setia presented a protocol for security of WSN. The name of the protocol is Localized Encryption and Authentication protocol (LEAP). This protocol used the different types of keys to secure the network and authenticate the node in the network. It uses the μTESLA technique for authentication of nodes. LEAP protocol uses four types of keys that are network key, group key, pairwise key and cluster key. These keys are used for different purpose and network key that is common for all nodes is used to generate the other keys after which this key is deleted from all nodes [9]. This protocol stops node compromise attack. This protocol is designed for key management and support in-network procession. A pair wise key is used for communication with neighbors nodes and a group key is used for group communication. Author analyze the protocol for different attacks and it is very effective against some attacks such as wormhole attack, node cloning and HELLO flood attacks. In 2009 Ling Tang and Ling Li propose the secure routing protocol that is the extension of SPIN [10] is known as S-SPIN (Secure- SPIN). This protocol works well against forgery attack ans operates in MAC layer. This protocol uses the rigorous mathematical technique and good for formal security framework. Routing Protocol for Low Power and Lossy Network (RPL) [26] is developed by ROLL working group in IETF. IETF is stand for Internet Engineering Task

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Force. This protocol operates on devices that have constrains on processing power and low energy. This protocol uses the directed acyclic graph (DAG) and set DIO for message broadcast. The purpose of this routing protocol is to be the IPv6 routing protocol for LLNs and sensor networks applicable to all types of LLN deployments and applications. The ROLL Working Group's official goal is to avoid heterogeneity in the sensor networking sector by providing an IP-based routing standard, and to gain wide industrial support behind this standard. Science 2011 there are many performance analysis and problems reported in this protocol include rank attack in 2013 and version number attack in 2017. In **2011** Amit Dvir, T´amas Holczer, and Levente Buttyan presents new challenges in RPL[11] . In RPL the rank of node is calculated and based on that routes are finding in the network. A malicious node can intentionally advertise a better rank. A rank attack is also identify that affect the performance of the node.

In **2014** authors in have enhanced the existing AODV protocol with some security extensions added to them and have put forth new protocol SE-AODV for efficient and secure routing [14]. This new SEAODV adds extra features to same AODV routing protocol making path formation more secure and followed by evaluation of proposed algorithm performance by comparing it to SAODV. But the major issue is how to detect and deal with a malicious node has been the key area of research. This has resulted in some scenarios wherein the node was malicious right from the beginning even before it joined the network, or initially it was a good node but after lapse of some time it has started its malicious activity, or maybe it pretends to be authentic but by helping another malicious node it is doing wrongful activities. None of possibilities can be identified in the beginning, unless the first packet is dropped at the node [17]. These adversary nodes give rise to various attacks like black hole attack, wormhole attack, sinkhole attack, jelly fish attacks etc that disrupts the network traffic. This results in high packet drop rate and eventually retransmission of the packets further results in network overhead. This results in the queuing mechanism to be implemented in manet too as discussed in [20].

In **2014** Also Even there are several reasons for the dropping of the packet and every packet drop at any particular node cannot be treated as the confirmation that the node is adversary node. Hence Detecting and Dealing with Malicious Nodes is a big problem in MANET. Similarly effect of varying node mobility can be predominantly seen in the analysis of the various routing algorithms [18].

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

In **2015** a survey of different scenarios suggests various attacks, their bifurcation in wireless networks and efforts need to be taken for their analysis under different scenarios in [19]. Due to installation in open environment Wireless networks are more vulnerable for attacks and more research should be done in the area of security. More secure and inelegant techniques are required to make a safe wireless sensor network. Apart from the nature of the attacks there is another view point that needs to be considered. At different layers the nature of attacks vary so their solutions [18, 19]. So no particular protocol will be able to provide a complete solution. To identify malicious is also very difficult. In the presence of malicious node the working of network is affected and a robust security solutions is required to protect the WSN from different types of attacks in totality. In 2016 Sudhakar Pandey, Deepika Agrawal and Muni Vijay gives a improved MRSPIN for health monitoring [36]. In healthcare domain for a sensor is very important to transmit reliable data in time. In SPIN protocol a timer is introduced that keep track the time and selective repeat if required and a reliable system may be develop using this technique. For health monitoring the Quality of Service (QoS) and quality of data is very important. A reliable system takes care all parameters like throughput, packet delivery ratio and energy used.

TinySec is the complete framework for security in wireless network that provide integrity access control and confidentiality [21]. TinySec uses RC5 for security. Symmetric key cryptography is used in this protocol. In [22] rekeying mechanism using hash chain and Elliptic Curve Cryptography.

6. Conclusion and future scope:

There is a lot of literature available and the limitations and uses of the sensor network are given in great detail. The sensor network technology's real success depends primarily on its application to remove a harmful situation or to maintain a good one. One of the major challenges is designing an effective and secure protocol and the sensor network problems depend on the application. Monitoring air quality is a prospective technology domain that is of particular value to our community. Major sources of air pollution are large cities with high concentration of manufacturing, complex transportation networks and high population density. The security technique apply in wireless sensor network can also be used in IoT network with modification. An IoT network is also a collection of sensors and interconnected devices and controlling devices. To authenticate the device and transfer the data securely is a major challenge in these networks.

7. References:

[1] Gong, Hang Long, Feihong Dong, Qing Yao, "Cooperative security communications design with imperfect channel state information in wireless sensor networks", IET Wireless Sensor Systems, Vol. 6, Issue: 2, pp. 35-41, 2016.

[2] Agnihotri, Ram Bhushan, Ajay Vikram Singh, and Shekhar Verma. "Challenges in wireless sensor networks with different performance metrics in routing protocols." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1- 5. IEEE, 2015.

[3] Jun Wu, Kaoru Ota, Mianxiong Dong, Chunxiao Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, Vol. 4, pp. 416- 424, 2016.

[4] Goutam Mali, Sudip Misra, "TRAST: Trust-Based Distributed Topology Management for Wireless Multimedia Sensor Networks", IEEE Transactions on Computers, Vol. 65, Issue: 6, pp. 1978-1991, 2015.

[5] Karlof C., and D. Wagner. May 2003. "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures." In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 113-127, Anchorage, Alaska, USA.

[6] Newsome, J., E. Shi, D. Song, and A. Perrig. 2004. "The Sybil Attack in Sensor Networks: Analysis and Defenses." In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 1259-1268.

[7] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," March 2011, Internet Draft, work in progress, draft- ietf-roll-rpl-19.

[8] S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[9] Sam Blackshear Rakesh M. Verma "R-LEAP+: Randomizing LEAP+ Key Distribution to Resist Replay and Jamming Attacks" SAC'10 March 22-26, 2010, Sierre, Switzerland. ACM 978-1-605 -638-0/10/03 2010

[10] Liang Tang QiaoLiang Li "S-SPIN: A Provably Secure Routing Protocol for Wireless Sensor Networks" International Conference on Communication Software and Networks 2009

[11] Amit Dvir, T´amas Holczer, Levente Buttyan, "VeRA - Version Number and Rank Authentication in RPL" Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems 2011

[12] Jitender Grover1, Shikha Sharma Security Issues in Wireless Sensor Network - A Review Department of Computer Science & Engineering, M. M. University, Sadopur, Ambala, India 978-1-5090-1489-7/16/$31.00 ©2016 IEEE

[13] Subrata Sahana, Karan Singh, Rajesh Kumar and Sanjoy Das A Review of Underwater Wireless Sensor Network Routing Protocols and Challenges Springer Nature Singapore Pte Ltd. 2018

[14] R. S. Shaktawat ,D. Singh ,N. Choudhary, "An Efficient Secure Routing Protocol in MANET Security – Enhanced AODV (SE-AODV) ", International Journal of Computer Applications, Vol.97, No.8, pp.1-12, 2014.

[15] Vikas Goyal and Geeta Arora, "Review paper on security issues in mobile Adhoc networks," International Research Journal of Advanced Engineering and Science, Volume 2, Issue 1, pp. 203-207, 2017.

[16] Pantazis, Nikolaos A., Stefanos A. Nikolidakis, and Dimitrios D. Vergados. "Energy-efficient routing protocols in wireless sensor networks: A survey." IEEE Communications surveys & tutorials 15.2 (2013): 551-591.

[17] A. K. Gupta, D. Mehrotra, "Detecting and Dealing with Malicious Nodes Problem in MANET"- International Journal of Scientific & Engineering Research, Vol.4, Issue.7, pp.61-68, 2013.

[18] A. Vijayan, T. Thomas, "Anonymity, Unlinkability and Unobservability in Mobile Ad Hoc Networks", International Conference on Communication and Signal Processing, India pp.3-5, 2014.

[19] G. Kalpana, S. Archana, "Performance Analysis of Threshold Based Algorithms under Wormhole Attack in MANET", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.133-138, 2015

[20] PK. Sharma, SL. Mewada, P. Nigam, "Investigation Based Performance of Black and Gray Hole Attack in Mobile AdHoc Network", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.4, pp.8- 11, 2013.

[21] Karlof, C., Sastry,N. Wagner,D. "TinySec: Link Layer Security Architecture for Wireless Sensor Networks," Sensys., Baltimore, MD 2016.

[22] Ummer Iqbal Sana Intikhab "Re-Keying Mechanism for TinySec using ECC and Hash Chains" International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Jan. 06 – 07, 2017

