International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10389-10393
© Research India Publications
http://www.ripublication.com

A Survey on Various Methods Used To Detect Attacks on Wireless Sensor Networks

Anjali Ramakrishnan, Alish Preethi

Abstract

This survey is based on the various methods that have been implemented in wireless sensor networks for detecting and preventing different attacks that are susceptible to wireless networks. WSNs are a large network that consists of many sensor nodes and sink nodes, where the packets are being forwarded from the source node to the destination node. However such networks are susceptible to attacks such as impersonation attack, capture node attack etc. This survey paper analysis the various techniques that has been used for detecting such attacks, throwing light on the advantages and disadvantages of these methodologies.

Introduction

Security is an essential requirement in wireless network to provide secure communication between the nodes in order to transfer data. In wireless sensor networks the nodes monitor the surrounding and pass on information to the corresponding nodes via multihop, relaying the message to the sink. Disaster response, weather observation, crime prevention, and healthcare systems are examples of applications where WSNs are utilized. The main issue with such network is that they are prone to various attacks such as node capture attack, eavesdropping, falsified packet insertion attack and impersonation attack. To overcome these drawbacks many techniques have been developed which will be analyzed in this survey paper.

Literature Survey

To analyze the effects of different kinds of wireless attacks in wireless sensor networks a survey has been conducted and discussed. This survey gives a brief description of the various existing and established theories.

DeepikaKukreja and MohitMiglani used dynamic source routing as the principle protocol which mainly consists of two components namely watchdog and pathrater which can analyze the path and detect the malicious node. The security enhanced DSR selects the most trustworthy path between source and destination that is free from malicious nodes.

Manjuprasad B and Andhe Dharani have presented a simple secure protocol for wireless sensor networks with a uniform clustering mechanism. An efficient clustering algorithm is used for efficient information transmission which can reduce the amount of memory consumed and make the nodes work efficiently during transmission of packets.

Fang Li and Pan Xiong have proposed a heterogeneous online and offline signcryption scheme in order to gain a protected communication between the sensor node and an internet host in order to accomplish integrity, confidentiality and authentication at a lower cost.

Vishnu Priya.P and Thanapal.P introduced an Intrusion detection system mainly used to detect blackhole attack that has the tendency to drop packets that are sent back to the host from the server. Inter domain filters are used to drop unsolicited packets. Unauthorized access can be avoided using this method.

A probabilistic misbehavior detection scheme called iTrust was proposed by Haojin Zhu, Suguo Du, Mianxiong Dong and Zhenfu Cao .The iTrust scheme makes use of a trusted authority to evaluate the node behavior. This methodology is able to attain reduced transmission overhead sustained by misbehavior detection.

TziporaHalevi, Haoyu Li, Di Ma, NiteshSaxena, Jonathan Voris and Tuo Xiang presented a method to deny unauthorized reading and an ideal defense mechanism which is incorporated with sensing technique for relay attacks in radio frequency identification systems. This system consists of a number of tags that carry valuable information making it prone to illicit access.

Kang Chen, Haiying Shen and Haibo Zhang has created a social network based P2P content file sharing system in disconnected mobile ad hoc networks. SPOON considers both node interest and contact frequency for efficient file sharing.An interest extraction algorithm is used to determine the interest of nodes for content based file searching.

MarkkuAntikainen, Tuomos Aura and MikkoSarela have developed aSource routed protocols where bloom filter is embedded with each packet in order to form the delivery tree.The nodes present in the network forward packets solely based on this packet information without cross checking the routing tables.

Gaojie Chen, Zhao Tian, Yu Gong, Zhi Chen and Jonathon A. Chambers haveproposed a relay selection policy of maximum ratio for secure buffer-aided cooperative decode and forward networks.The best relay is selected with the help of the buffers present in the relays. This significantly improves the performance when it comes to secrecy outage probability.

Zhiguo Shi, Ruixue Sun, Rongxing Lu and Xuemin Shen have proposeda secure neighbor discovery scheme which is resistant to wormhole attacks.RDMA protocol is utilized here to prevent collision of nodes present in the network. The SND scheme has proved to be very effective when it comes to detecting wormhole attacks.

S.no	Author	Title	Algorithm	Parameters	Remarks
1	Deepika Kukreja. et.al., (2014)	Security enhancement by detection & penalization of malicious nodes in WSN	Dynamic source routing (DSR) & security enhanced DSR.	• Packet delivery ratio is high. • Packet loss percentage is low. • Average end-to end latency is low.	Rise in packet overhead.
2	Manjuprasad B &Andhe Dharani. (2014)	Simple secure protocol for wireless sensor networks.	Uniform clustering algorithm.	• Communication overhead reduced.	Further improvement needed on security.
3	Fagen Li & Pan Xiong (2013)	Practical secure communication for integrating WSN into Internet of Things	A heterogeneous online & offline signcryption scheme	• Security is maintained	Heterogeneous signcryption are only secure against outsider attacks.

S.no	Author	Title	Algorithm	Parameters	Remarks
4	VishnuPriya.P& Thanapal.P (2013)	Intrusion detection System against Blackhole attack in wireless networks	Intrusion detection system which uses inter domain filters to drop unwanted packets.	• Node registration & connection. • Node frame creation. • Blackhole guard	This methodology is well suited for heterogeneous wireless network models.
5	Haojin Zhu.et.al., (2014)	A Probabilistic misbehavior detection scheme towards efficient Trust establishment	A Probabilistic misbehavior detection scheme (iTrust) which can reduce the	• Scalability is good. • Packet loss rate has little effect on the performance	High transmission & signature verification overhead.

		in Delay Tolerant Network.	detection overhead effectively	of iTrust. • Node mobility is high.	
6	Tzpora Galevi.et.al., (2014)	Context-aware defenses to RFID Unauthorized reading & relay attacks.	Context aware selective unlocking &Transaction verification using sensor data correlation.	• Data collection. • Performance of similarity detection technique	This methodology cannot guarantee absolute security and usability.
7	Kang Chen.et. al., (2014)	Leveraging social networks for P2P content based file sharing in disconnected MANETs.	SPOON algorithm	• Higher hit rate. • Lower average delay.	Low hit rate and higher average delay may arise if node churn consideration is not considered.
S.no	**Author**	**Title**	**Algorithm**	**Parameters**	**Remarks**
8	Gaojie Chen.et. al., (2014)	Max-ratio relay selection in secure buffer aided Cooperative wireless networks.	Max ratio selection scheme which optimizes secrecy transmission.	Secrecy outage probability is improved.	These protocols cannot detect replication attacks in mobile sensor networks
9	Markku antikainen.et.al., (2013)	Denial -of - service attacks in bloom filter-based forwarding.	Source routed algorithm.	Injection attack efficiency	Such protocols make fake security assumptions.
10	Zhiguo Shi.et.al., (2014)	A wormhole attack resistant neighbor discovery scheme with RDMA protocol for 60Ghz directional network.	Wormhole attack resistant SND scheme	• Back off mechanism of the RDMA protocol. • NC strategies.	High propagation loss due to high carrier frequency.

Conclusion

In this paper we have come across various techniques to detect and prevent attacks in wireless sensor network. Wireless technologies use the air as the physical media when sending and receiving data packets making it prone to various wireless attacks. Although some of these methods have proved to be very efficient in accomplishing prevention of such harmful attacks, few of these methodologies have disadvantages which must be properly analyzed in order to overcome this fault.

References

[1] "Security enhancement by detection & penalization of malicious nodes in WSN", 2014 international conference on SPIN (signal processing & integrated networks).

[2] "Practical secure communication for integrating WSN into Internet of Things", 2013 IEEE sensors journal, vol.13.

[3] "Intrusion detection System against Blackhole attack in wireless networks", International journal of computer Applications & information technology, vol.2, 2013.

[4] "A Probabilistic misbehavior detection scheme towards efficient Trust establishment in Delay Tolerant Network", IEEE transaction, vol.25, 2014.

[5] "Leveraging Social Networks for P2P Content-Based File Sharing in Disconnected MANETs", IEEE transaction, vol.13, 2014.

[6] **"**Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks", IEEE transactions on information forensics and security, vol. 9, 2014.

[7] "A wormhole attack resistant neighbor discovery scheme with RDMA protocol for 60GHz directional network", IEEE transaction, 2014.

[8] "Simple secure protocol for wireless sensor networks", IEEE paper 2014

[9] "Context-aware defenses to RFID unauthorized reading and relay attack", IEEE transaction in emerging topics in computing, 2012.

[10] "Denial-of-Service Attacks in Bloom-Filter-Based Forwarding", IEEE/ACM transaction on networking, 2013