A Survey on Intrusion Detection Techniques in Wireless Sensor Networks

Swati Kasar
PG Student [Communication Network],
Dept. of E&TC, D.Y.Patil College of Engineering,
Akurdi, Pune

Trupti Wagh
Assistant Professor,
D.Y.Patil College of Engineering,
Akurdi, Pune

ABSTRACT
This paper discuss various techniques of intrusion detection in wireless sensor networks available. This paper gives an introduction to wireless sensor networks, security in WSN and describe various techniques used to overcome attacks. The prevention techniques according to the network structure of WSN and a convenient method of intrusion detection and prevention in wireless sensor networks are studied in this paper. Thus, the papers main aim is to include the most recent advancements in this area as well as to predict the future course of research so that the general as well as expert readers could be greatly benefited.

Keywords
Wireless Sensor Networks, Intrusion detection.

1. INTRODUCTION
Wireless sensor networks are the network of spatially distributed sensors (as shown in figure 1) to monitor physical conditions of an environment like temperature, pressure, sound etc. WSNs consist of sensor nodes and sinks. They are self healing, self organizing, decentralized and distributed in nature. Communication in WSNs takes place through multi-hop sensor nodes. The main objective of a sensor node is to collect information from its surrounding environment and transmit it to the sink. WSNs have wide range of application like in climate detection, monitoring different environments and in military applications. These networks are wireless and are deployed in physical harsh and hostile environments in which the nodes are always exposed to physical security damages. The characteristics of WSNs are self organizing nature, low battery power supply, limited bandwidth support, distributed operations in wireless environment, multi-hop communication and dependency on other nodes. The characteristics are responsible for security attacks on all layers of the OSI model.

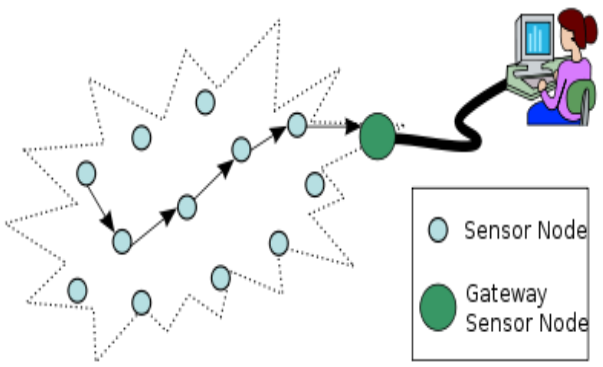

Figure 1 Basic Wireless sensor network architecture

2. SECURITY IN WSN
The limited resources of wireless sensor networks and applications of WSN in harsh environments lead to security problems in wireless sensor networks. Security in WSNs is a serious concern. Security in WSNs faces many challenges because of broadcast nature of WSN, limited resources, vulnerability to physical attacks etc. Various techniques used for security purpose include key management, cryptography, secure routing, security mechanisms for specific attacks and various IDS (Intrusion detection systems). Cryptography and key management alone cannot handle the attacks in WSNs hence; various IDS are used. IDS are the defense systems used in WSNs for security. IDS are one possible solution to eliminate various attacks in WSNs. IDS is also known as second line of defense. IDS can detect attacks but cannot prevent them or respond to them. Hence only used for intrusion detection. IDS alarm the controller to take action against attacks.In this paper, various possible existing solutions for preventing attacks in WSNs including IDS, key management are discussed. Various IDS are reviewed and comparison is made discussing their functions in intrusion detection in WSN.

3. VARIOUS SECURITY TECHNIQUES IN WSN
IDS are classified into two main important classes one is rule based IDS and second is anomaly based IDS.[2] Rule based IDS is also known as signature based IDS which is used to detect intrusions with the help of built in signatures. It detects well known attacks with accuracy but does not detect an attack for which signatures are not present in the intrusion database. In anomaly based system the traffic patterns are matched or resource utilizations. These IDS detect well known and new attacks but also have more false alarms. Some IDS operate with a specific routing protocol, like proactive and reactive protocols. These protocols help in finding the most reliable path from source to destination.

The hybrid intrusion detection systems are combination of anomaly based and signature based systems. It consists of two modules one module is used for detecting well known attacks using signatures while the other module is used for learning and detecting normal and malicious patterns and studies deviation from normal patterns. Hybrid systems are more accurate but consume more energy and resources. Hence it is not recommended for a resource constraint networks like WSNs. Other hybrid systems are SVM (State vector machine) and misuse detection.

As a multi-hop wireless network WSNs are vulnerable to multi-layer attacks. Security mechanism for one layer cannot protect and respond to attacks in another layer. Cross layer IDS are capable of detecting multilayer security attacks. Cross layer IDS are also not considered for a resource constraint WSNs because

this IDS exchange parameters across the protocol stake which consume more power memory and processing. Cross layer intrusion detection agent (CLIDA) for WSNs ensures cross layer exchange of information amongst physical, MAC and network layer. Cross layer data module collects an represents data to all layers. CLIDA is capable of detecting multi-layer security attacks.

Anomaly-based IDSs are suitable for small-sized WSNs where few nodes communicate with the base station. In small sized WSNs, the traffic pattern is mostly the same, so unusual traffic pattern or changing behavior can be treated as an intrusion. However such IDS may generate more false alarms and may not be able to detect well-known intrusions. Anomaly-based IDSs are usually lightweight in nature and mostly use statistical, probabilistic, traffic analysis or intelligent techniques.

Signature-based IDSs are suitable for relatively large sized WSNs, where more security threats and attacks can compromise network operations. Signature based IDS needs more resources and computations as compared to anomaly based IDS. One of the important and complex activities is the compilation and insertion of new attack signatures in the databases. Such IDSs mostly use data mining or pattern matching techniques.

Hybrid IDSs are suitable for large and sustainable WSNs. These IDSs have both anomaly-based and signature based modules, so they require more resources and computations. To reduce the usage of limited resources, such mechanisms are mostly used in cluster based or hierarchical WSNs, in which some parts of the network are used to execute anomaly detection while other parts are accompanied with signature, based detection. Cross layer IDSs are usually not recommended for a resource constraint networks such as WSNs, as it consumes more resources by exchanging parameters across the protocol suits for attack detection.

Key management in a large cluster based sensor network with limited resources is a challenging task[1]. An attacker can compromise the entire network security just controlling few nodes and injecting false data in an undetected manner. To protect WSNs from such impersonating attacks a dynamic key management framework particularly for large-scale clustered sensor networks is used. In framework different keying mechanisms like secure in-cluster, inter cluster and individual communication by refreshing keys on demand while adaptively handling node addition and capture. Security in cognitive wireless sensor networks (CWSN) is an important problem because these kinds of networks are used in critical and important applications[1]. Moreover, the limited resources of WSN make the problem even more complex. PUE attack detection in CWSN using collaboration and learning behavior is used. Here focus is on primary user emulation (PUE) attack in CWSN. In PUE attack, a malicious node emulates the behavior of an incumbent node to use the radio spectrum for its own useless operation or stop the other nodes to access the spectrum.

External attacks can be detected easily as compared to internal attacks. In internal attacks, the attacker is inside and most of the time is a legitimate member of the network. Detection and prevention of selective forwarding based denial of service attacks in WSNs is a mechanism to detect insider malicious node capable of selective forwarding based denial of service attack. The scheme uses trust management approach to detect such malicious nodes and their victims.

Adaptive ant based[2] secure routing protocol is to select two optimal paths keeping in view route security. Secure ant based routing protocol for wireless sensor network scheme has four important steps that is, route discovery, route selection, route security, and data forwarding to destination. This mechanism is inspired from the real ants. Forward and backward ants are used for route request and route reply purpose. The forward ants collect and increment the reputation values along the path to ensure security. Lightweight intrusion detection: modeling and detecting intrusions dedicated to OLSR protocol is a signature based IDS in cooperation with OLSR routing protocol.

A general mechanism called packet leashes is used for detecting and thus defending against wormhole attacks and a specific protocol called TIK that implements leashes is used. A lightweight countermeasure for the wormhole attack called LITEWORP does not require specialized hardware. LITEWORP is particularly suitable for resource constrained multi-hop wireless networks, such as sensor networks. This allows detection of the wormhole, followed by isolation of the malicious nodes.

Checkpoint based Multi-hop Acknowledgement Scheme; CHEMAS[8] is a lightweight security scheme for detecting selective forwarding attacks. This scheme can randomly select part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. An Intrusion-tolerant routing protocol for wireless Sensor Networks (INSENS)[9] constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station.

In "An Energy-Efficient Routing Method with Intrusion Detection and Prevention for Wireless Sensor Networks",[1] two types of schemes are applied, heavy communication overhead and resulting excessive energy consumption of nodes occur. Energy efficient routing method in an environment where both intrusion detection and prevention schemes are used in WSNs.

4. CONCLUSION

In this paper, we discuss various security mechanisms used for security in wireless sensor networks. Also we discuss key management techniques, various intrusion detection systems (IDS) and combination of two schemes for intrusion detection and prevention. An extensive review is done on various types of IDS. Discussing their drawbacks and types of WSN for which each of one is suitable. We come across a need for intrusion detection as well as prevention in wireless sensor networks. Hence through this survey it can be concluded that the combination of two schemes can be used to overcome various drawbacks.

5. REFERENCES

[1] Abduvaliyev, A.; Pathan, A.-S.K.; Jianying Zhou; Roman, R.; Wai-Choong Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," Communications Surveys & Tutorials, IEEE , vol.15, no.3, pp.1223,1237, Third Quarter 2013

[2] Research Article Intrusion Detection Systems in Wireless Sensor Networks: A Review Nabil Ali Alrajeh, S. Khan, and Bilal Shams, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 167575.

[3] Intrusion Detection and Security Mechanisms for Wireless Sensor Networks S. Khan, Jaime Lloret, and Jonathan Loo,

Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 747483

[4] Soo Young Moon; Ji Won Kim; Tae Ho Cho, "An energy-efficient routing method with intrusion detection and prevention for wireless sensor networks," Advanced Communication Technology (ICACT), 2014 16th International Conference on , vol., no., pp.467,470, 16-19 Feb. 2014

[5] Karlof, C.; Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures," Sensor Network Protocols and Applications, 2003. Proceedings of the first IEEE. 2003 IEEE International Workshop on, vol., no., pp.113,127, 11 May 2003

[6] Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks," INFOCOM 2003. Twenty-Second Annual Joint Conferences of the IEEE Computer and Communications. IEEE Societies, vol.3, no., pp.1976,1986 vol.3, 30 March-3 April 2003

[7] Khalil, I.; Bagchi, S.; Shroff, N.B., "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, vol., no., pp.612,621, 28 June-1 July 2005

[8] B. Xiao, B. Yu and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks", published in IEEE journal of Parallel and distributed computing, Vol.67, No.11, pp.1218-1230, 2007.

[9] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks", published in international conference of Computer communication, Vol.29, No.2, pp 216-230, 2006.

[10] Fan Ye; Haiyun Luo; Songwu Lu; Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on , vol.23, no.4, pp.839,850, April 2005

[11] Akyildiz, I.F. Weilian Su; Sankarasubramaniam, Y. Cayirci, E, "A survey on sensor networks," Communications Magazine, IEEE , vol.40, no.8, pp.102,114, Aug 2002

[12] Butun I, Morgera, S.D, Sankar R, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," Communications Surveys & Tutorials, IEEE, vol.16, no.1, pp.266,282, First Quarter 2014

[13] Bashir, U.; Chachoo, M., "Intrusion detection and prevention system: Challenges & opportunities," Computing for Sustainable Global Development (INDIACom), 2014 International Conference on , vol., no., pp.806,809, 5-7 March 2014

[14] Roman, R.; Jianying Zhou; Lopez, J., "Applying intrusion detection systems to wireless sensor networks," Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE , vol.1, no., pp.640,644, 8-10 Jan. 2006

[15] Techateerawat, P.; Jennings, A., "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks," Web Intelligence and Intelligent Agent Technology Workshops, 2006. WI-IAT 2006 Workshops. 2006 IEEE/WIC/ACM International Conference on , vol., no., pp.227,230, 18-22 Dec. 2006