International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Survey on Insider Threats Security in Wireless Ad-Hoc Networks

T.Vadivu[1], Dr.D.Radha Damadoram[2]

[1]*Research Scholar, CMS College of Science and Commerce, Coimbatore, Tamil Nadu,(India)*

[2]*Associate Professor, CMS College of Science and Commerce, Coimbatore, Tamil Nadu, (India)*

ABSTRACT

Wireless sensor networks are used for the protection of the false data and network connections between the nodes. In recent years Wireless ad hoc networks (WANETs) can be classified as Insider and Outsider threats. This article focus on Insider threats which comes from the users who are fully authorized to access the systems which they are using. In this paper, Security attacks and protocols used is mainly focused in WSNs with intrusion techniques. Cryptographic techniques of routing protocols and security requirements are presented.

Keywords: Security protocols, Wireless sensor networks, Routing protocols, Intrusion, WANETs.

I.INTRODUCTION

A Wireless Ad-Hoc network consists of mobile platforms which are free to communicate without any central control entity [1]. It is defined as a collection of nodes that communicate each other wirelessly by using radio signals with a shared common channel. It can operate in an isolated manner or with fixed networks through gateways. The power of an ad hoc network is that it does not differentiate between a router and a station, i.e., each station contributes to routing. The WANET is an autonomous system of mobile nodes, which has several salient characteristics namely, dynamic topologies, bandwidth-constrained and energy constrained operation, and limited physical security [2]. At the same time, however, ad hoc social networks are getting increasingly important which takes the human factors into consideration, i.e., human mobility, human selfish status, and human preferences. This survey focuses on wireless ad hoc networks (WSNs). It can be used with many applications due to its sensing capabilities, CPU power and radio transceiver with plenty of sensor devices. Power source is limited so that nodes comprised by the network are often battery-fed devices. Also the network throughput is limited. Conventional networks with fixed infrastructure require protection against injection or modification of disseminated data packets and eavesdropping. Most applications of WSNs require the same protection. The wireless medium and sensor networks are vulnerable to security attacks. Thus the insider and the outsider can monitor the network, easily access and launch the attacks.

The remaining of this article is organized as follows: In Section 2, reviews on some insider attacks regarding wireless sensor networks and some routing protocols with cryptographic techniques is discussed. In section 3, characteristics and features of wireless sensor networks is discussed. In section 4, the routing services and insider attacks by providing a false node is discussed. In section 5, the cryptographic protocols for the issues of trust based routing is discussed. In section 6, research work is concluded.

II.LITERATURE REVIEW

In [3] P.Sengar, N.Bhardwaj "A Survey on Security and various Attacks in Wireless Sensor Networks" provides the essentials about various insider threat attacks which exist in the wireless sensor networks such as Passive Attack, Active attack, Insider attack and Outsider attacks are discussed. In this paper, the introduction of WSN, cryptographic techniques have been discussed.

In [4] Hsing-Chung Chen, "TCABRP: A Trust Based Cooperation Authentication Bit-Map Routing Protocol against Insider Security Threats in Wireless Ad Hoc Networks", this paper discusses the insider threats in WANETs. Also evaluation is done with three factors. Implementation is done with an efficient cryptographic routing protocol such as Trust based Cooperation Authentication Routing Protocol which is a behavioral based technique.

In [5] Wenjuan Li, Weizhi Meng, Lam-For Kwok, Horace H.S.IP , " Enhancing Collaborative Intrusion Detection networks against insider threats using supervised intrusion sensitivity-based trust management model" describes about the malicious nodes which are utilized by the insiders and intrusion detection techniques to automatically assign the values. In evaluation supervised classifiers with trust model is used.

In [6] Matthias Hollick, Cristina Nita-Roaru, Panagiotis Papadimitratos, "Toward a Taxonomy and Attacker Model for secure Routing Protocols". This paper initiates the study of structured approach to secure routing protocols and the attacks. The routing system is decomposed into its key components based on a functional model of routing providing classification of attacks on secured routing protocols.

III.SECURITY CHARACTERISTICS FOR WANETS

Tab.1 specifies the characteristics of ad hoc network WANET in terms of Node, Dynamic Topologies, Bandwidth, Energy Constraints, Limited Physical Security, Hidden Terminals, Packet loss.

Characteristics	Impacts
Node	Nodes with energy
Dynamic Topologies	Node changes dynamically
Bandwidth	Less transmission rate. Collision occurs frequently.
Energy Constraints	Rely on batteries or other exhaustible energy
Physical Security	Physical threats than fixed cable networks
Hidden Terminals	Unknown attacks
Packet loss	Injected false data

Tab1. Impacts based on characteristics

IV. ROUTING COMPONENT ATTACKS

A different type of attackers with different kinds of functions is listed out here. These attacks are particularly harmful when framed by an insider attack. Main goal of an attack on the routing system is to influence the paths through which the packets are routed. In case, the attacker controls a route directly, it can be achieved by forwarding the packets to the wrong port for which the range and impact is usually limited. The attackers not only change the route but even the configuration of the other remote routers. In this section we discuss about the Transport service, Topology service, Routing Identity Attacks.

4.1 Transport Service

This transport service provides protection such as authentication, Integrity and Confidentiality.

Injection: An attacker may inject false packets into the communication channels which is used by the transport service in order to corrupt the data and also to exhaust the network.

Eavesdropping: An attacker may silently listen to the communication to learn about the confidential topological details.

Node compromise (Destruction or theft):

It includes the physical capturing of a node in sequence to disrupt network by breaking the communication path or reprogramming a node so that it acts as a spy in network.

4.2 Topology Service

The following dimensions can be attacked:

Database Attack: This attack is done directly by attacking the database by modifying it and also an attacker can divert traffic which harms confidentiality.

Radio Jamming: The attacker tries to disrupt the communication by sending few radio waves at the similar frequency resulting in interference or collisions of packets over network. Jamming can be intermittent or continuous depend on the time for which network is kept jammed.

Neighbor Discovery Attack: This is done by attacking the neighbors by creating warm holes generating some other nodes to the network.

4.3 Routing Identity Attacks:

Attacks on the route identity services include:

Black Hole Attack: A false node which tries to become the neighbor of the node for receiving the packets by altering their routing tables, so that the packets are not forwarded to the correct destination.

Selective Forwarding (Gray Hole Attack):A malicious node is inserted into the network which tries to change the routing and captures the data as black hole attack does. But this attack selectively forward data (not all). So detection of false node is difficult.

Wormhole Attack: This attack is done with at least two malicious nodes which have high bandwidth between them either wired or wirelessly. These malicious nodes will show other normal nodes that they provide the shorter path to the target even if they are lying far away in the network. So, the node will forward data to the malicious node that can be captured by attacker easily.

Sinkhole Attack : The malicious node reside near the BS and it tries to imaginary to be closest node to the BS so that other surrounding usual node will change themselves and forward info to the malicious node.

Sybil Attack: Attackers generate a huge number of identities to destroy the availability of the routing services by consuming excess resources.

V.CRYPTOGRAPHIC METHODS USED IN WANET'S

These protocols mainly focus on the issues of trust-based routing, mobility, power consumption and real traffic on the same routes. In this section we discuss about the cryptographic protocols with intrusion mechanisms such as Bit-map table driven protocol (BTDRP) [7], Trust-based cooperation bit-map routing protocol (TCBRP) [8], Cooperative trust bit-map routing protocol (CTBRP) [9], Collaborative Intrusion detection networks(CIDN) [5].

Bit-map table driven protocol (BTDRP): The agent node gathers the knowledge and creates the information topology bit-map. So the path of nodes can be easily calculated by the bit-map. AODV [7] is an efficient routing protocol for maintaining the overhead the routing bit-map table in ad hoc networks.

Trust-based cooperation bit-map routing protocol (TCBRP): They could not fully prevent the false injected nodes from the attackers. So trust-based cooperation bit map routing protocol is used to prevent the false nodes and the damages. Initially daemons like [4] trust agent[TA] node, node recovery daemon, nodes registration daemon, add, update and remove daemon with Route vector Authentication Code (RVAC) is used. So in TCBRP packet delivering using RVAC, light weight computations using ECC cryptographic pair, mission-based key management are the techniques used to prevent the injected false nodes from the insider attacks.

Cooperative trust bit-map routing protocol CTBRP: Protocol is used for ensuring the trusted routing table in order to reduce the damages from the insider threats. Genetic Algorithm (GA) is the evaluation technique used to evaluate the inside nodes which are fully authorized users to communicate with the WANETs and to find the malicious nodes with lower score values. The nodes send the packets from source to destination along with the cooperative trust route, which is a behavioral based technique. Once a relay node has been damaged or compromised by an insider threat, it will cause damage in other nodes. Therefore CTBRP [9] protocol not only evaluates the behavior but also reduces the damages of the node tN_k from the insider threats in the WANETs.

Collaborative Intrusion detection networks (CIDN): This detection accuracy enables IDS to collect the information and to evaluate the detection techniques. In evaluation, the performance of three different classifiers [5] with machine learning techniques is used such as k-nearest neighbors algorithm (KNN), back-propagation neural networks (BPNN), decision tree(DT). KNN operates on the classification of unknown instances.

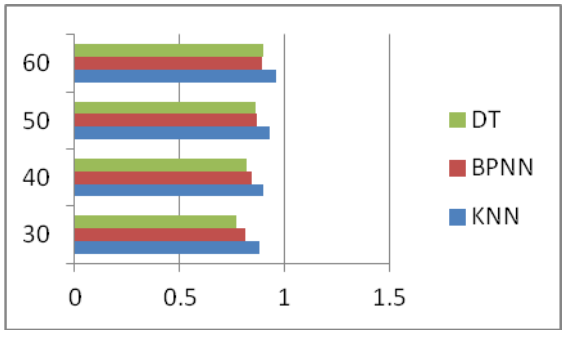

Fig 1: Classifiers: Accuracy Vs alarm values

BPNN is used to modify the error back-propagation with internal network weights. DT aims to classify the given datasets according to the values of its attributes.

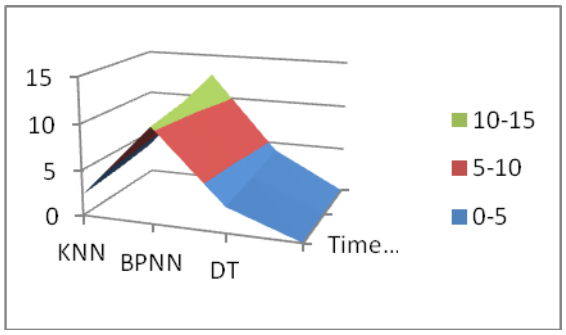

Fig 2: Classifiers: Time consumption Vs alarm numbers.

VI.CONCLUSION

The insider threats are actually the work of the authorized users to the WANETs communication system not the hackers. Therefore security features and factors of insider attacks are summarized. Table driven protocols based on the behavior and the issues of the trust-based routing such as Bit-map routing protocol with AODV is used and Cooperative trust bit-map routing protocol for n damaged nodes along with genetic algorithm is discussed. Trust based cooperation bit-map routing protocol with a trust agent and route vector authentication code is discussed. Intrusion sensitivity based trust management protocol CIDN with different levels of classifiers is used to evaluate the accuracy and time consumption values. Finally the protocols used in this paper are not only to evaluate the behavior but also to prevent the insider threats.

Journal Papers

[1.] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "*Wireless ad hoc networks*," Encyclopedia of Telecommunications, 2002.

[2.] I. Chlamtac, M. Conti, and J. J.-N. Liu, "*Mobile ad hoc networking: imperatives and challenges*," Ad Hoc Networks, *vol. 1, no. 1, pp. 13–64, jul 2003. [*Online].

[3.] P. Sengar, N. Bhardwaj, "*A Survey on Security and Various Attacks in Wireless Sensor Network*", 2017, IJCSE, Volume-5, Issue-4.

[4.] Hsing-Chung Chen, "*TCABRP: A Trust Based Cooperation Authentication Bit-Map Routing Protocol Against Insider Security Threats in Wireless Ad Hoc Networks*", IEEE vol 11,2 june 2017.

[5.] Wenjuan Li, Weizhi Meng, Lam-For Kwok, Horace H.S.IP , " *Enhancing Collaborative Intrusion Detection networks against insider threats using supervised intrusion sensitivity-based trust management model*", Elsevier ,journal of network and computer applications, 2017,135-145.

[6.] Matthias Hollick, Cristina Nita-Roaru, Panagiotis Papadimitratos, "*Toward a Taxonomy and Attacker Model from secure Routing Protocols*", ACM Sigcomm Computer Application review, Volume 47 Issue 1, Jan 2017.

[7.] H. Kim, S. Lee, and C. Kim, "*Design of knowledge discovery agent for a bit-map on Ad Hoc networks*," in Proc. 1st KES Int. Symp. Agent Multi Agent, Syst.: Technol. Appl., 2007, pp. 738–746.

[8.] H. C. Chen and J. Y. Lin, "*A trust-based cooperation bit-map routing protocol for Ad Hoc networks*," in Proc. 8th Int. Conf. BWCCA, Oct. 28–30, 2013, pp. 539–544.

[9.] H. C. Chen and H. K. Su, "*A cooperative trust bit-map routing protocol using the GA algorithm for reducing the damages from the InTs in WANETs*," J. Internet Services Inf. Security (JISIS), vol. 4, no. 4, pp. 52–70, Nov. 2014.

[10.] S. A. Kazarlis, A. G. Bakirtzis, and V. Petridis, "*A Genetic algorithm solution to the unit commitment problem*," IEEE Trans. Power Syst., vol. 11, no. 1, pp. 83–92, Feb. 1996.

[11.] D.E.Goldberg, "*Genetic Algorithms in Search, Optimization and Machine Learning, Reading*", MA, USA: Addison-Wesley, 1989.

[12.] M. Ahmad, M. Habib, and J. Muhammad, "*Analysis of security protocols for Wireless Sensor Networks*", in Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011, Shanghai, China, 2011, vol. 2, pp. 383–387.

[13.] Bao, F., Chen, I.R., Chang, M., Cho, J.H., 2012. "*Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection"*. IEEE Trans. Netw. Serv. Manag. 9 (2), 169–183.

[14.] Meng, W., Li, W., Kwok, L.F., 2015. "*Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection*". Secur. Commun. Netw., 8(18), 3883–3895 (Wiley).

[15.] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen. Becan: "*A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems*", 23(1):32–43, January 2012.