Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100196, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

To Enhance the Security in Wireless Nodes using Centralized and Synchronized IDS Technique

Ravi Shanker, Ashish Kr. Luhach* and Amit Sardar

Department of Computer Science and Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India;
ravishanker20@gmail.com, ashishluhach@acm.org, amit.cse.imps@gmail.com

Abstract

Objectives: Wireless technologies enable devices to communicate without any guided medium. It uses radio frequency for transmitting data, where the wired technologies use cables. It is mostly used to refer a telecommunications network that is interconnected between nodes and implemented without any kind of wires like as a computer network. Due to unguided media it's very tedious to detect any intrusion during communication. The aim of this work is to develop an approach which will detect and prevent black hole attacks so the any unauthorized or unwanted nodes if participates in the communication process will be detected in the real time. **Methods/Statistical Analysis:** In our work we are going to propose IDS which will helps to provide security to detect attacks and to prevent the attacks. Centralize and synchronized IDS node will work on the basis of anomaly detection technique. It will create pattern for malicious activates and do event detection on the basis of anomaly detection. **Findings**: The proposed method will enhance the detection of anomaly detection techniques with synchronized IDS within the cluster as well as between the clusters with the help of DRI table. **Application/Improvement:** This technique will helps to enhance security in Wireless network and helps to make more reliable network for user.

Keywords: Attacks, Anomaly, Cluster, Intrusion Detection System, Malicious

1. Introduction

A wireless network is any type of network http://en.wikipedia.org/wiki/Computer_network that uses wireless data connections for connecting nodes. It enables people to access and communicate to other devices without any need of wires. Wireless network allows the people to browse the internet from any location. Wireless network is defined in many types.

In case of active attacks, data integrity is break. As the attacker modified the data and sends to the user. Intrusion is an action that is meant to compromise the message integrity that include modification the data, availability of the resource such as DoS attack, repudiation of data by denying it, authentication by accessing using unauthorized identity and confidentiality which include reading of message by deciphering it. The reason behind all this is due to deficient in trust between the neighbors or nodes within the network. It monitors the activities in the network and gathers data to find whether the system has been compromised under attack. Installation of network intrusion detection system in MANET helps in indicating who has committed the attacks. Behavior of the neighboring node is analyzed by intermediate node in intrusion detection system. Once the faulty node is traced, it is taken away or removed from the network environment and alert message is communicated to all the neighboring nodes connected in the present network. In the proposed scheme it uses the intrusion detection technique to detect the malicious activity in the network by using DRI table and trust level. Several authors have proposed their method in context of the above statement. In[1], explores the use of clock skew which is used in WLAN access point as its finger print to detect unauthorized access points quickly and precisely. In this paper they calculated

*Author for correspondence

the clock skew synchronized with client and an access point from the IEEE 802.11 TSF time stamps which is transferred in the beacon or probe response frames. In[2], proposed a new technique of fake access point identification method to solve the access point related problems at the client-side. This technique uses the received signal strengths (RSS) and online detection algorithm.

In[3], proposed a method for detecting session hijacking attacks which calculates received signal strength and do the analysis on the basis of wavelet. This paper described the changes in the RSS of the channel can be done during a session hijack. To detect this session hijack[4] designed an optimal filter for detecting the intrusion. In[5] , proposed that when sending association and disassociation frame, it is sent in an unencrypted form which an intruder can capture and change the frame in between. On the LAN system[6] conducted this experiment and developed an information capturing techniques to gain Cookies and Session identity inside Cookies. Another set of solution presented in[7,8] is cross-site scripting which is at server site by mitigating the vulnerability in the web page scripting language. In[9,10], elaborated many web applications exposed to the likelihood of being attacked to session hi-jacking attacks due to the inappropriate use of cookies for managing the session. In[11] proposed One-Time Cookies (OTC) for implementing HTTP session authentication protocol that is efficient, easily deployed and is proof against session hijacking. In[12,13], conducted the experiment and found some critical output of the experiment about security level of some well known web mails like Gmail, Hotmail and Yahoo. With the help of Session Hijacking these three Web Mails were hacked.

2. Proposed Work

A Black Hole attack is also called as a packet drop attack where the malicious node will drop the received packet which affects the network throughput. The nodes are grouped together to form the clusters and each cluster has a cluster-head. It will collect the all information of every node inside the network and forward to the IDS node. Clustering is used to improve the lifespan of the nodes. If a network is under a black hole attack, when the source node broadcasts to all neighboring nodes in the cluster with the route request message, then the black hole instantly replies with the route reply message having very short interval of delay compared to the original route request message from destination node to the source node. The IDS will work using anomaly detection technique. So in the anomaly detection technique we used some parameter to detect the intrusion properly. We used some parameter like DRI (Through From) table, loss rate (mean how many packets were lost per node in previous transmission), Transmission rate (mean how many packet were successfully transmitted), Trust rate (that will provide by neighbor nodes), Packet drop ratio, communication between one node with all other nodes, communication access time, communication delay. By using this parameter the IDS will detect the intrusion. It is expected that the proposed technique will detect intrusion which can effect. It can prevent the intrusion attack also. It will also help to inform the cluster about its nodes that any node is black hole here or not.

There are various techniques are in literature which are used to prevent attacks. But here we are going to propose IDS which will helps to provide security and to prevent attacks. Centralize and synchronized IDS node will work on the basis of anomaly detection technique. It will create pattern for malicious activates and do event detection on the basis of anomaly detection technique. First of all, the cluster head is created and luster heads will synchronize information from IDS node standard wireless protocol. Formation of cluster heads will be on the basis of k-means clustering. After cluster is created the neighbor node is communicates with each other. In figure 1, X and Y represent node 1 and node 2 between which communication will takes place.

2.1 Algorithm

1. Initialize random nodes Node 1, Node 2,….Node n.
2. Apply k-means clustering to divide area into clusters.
3. Select cluster head on the basis of highly residing energy into nodes.
4. The node with highest energy will be cluster head in every cluster.
5. Deploy centralize IDS node and synchronize it with every cluster head using 802.11 Wi-Fi standard.
6. Do anomaly detection and create a table which is given below.
7. Node 1 wants to communicate with node 2
8. Node 1 sends request message to its cluster head.
9. Cluster head collect information from IDS node. IDS will check the DRI table that FROM value is one or not. If one mean it drop packet and based up on

that IDS send an alert message to Node 1 else forward to respective node.
10. On the basis of alert message, Node 1 will communicate with node 2.
11. If Alert message is normal then Node 1 will communicate with Node 2.
12. Else drop the packet.

Table 1. Detection Table

IDS				
NODE ID	DATA ROUTING TABLE		TRUST RANK	USAGE
	FROM	THROUGH		
1	1	1	8	20%
2	0	1	6	15%
3	0	0	1	65%

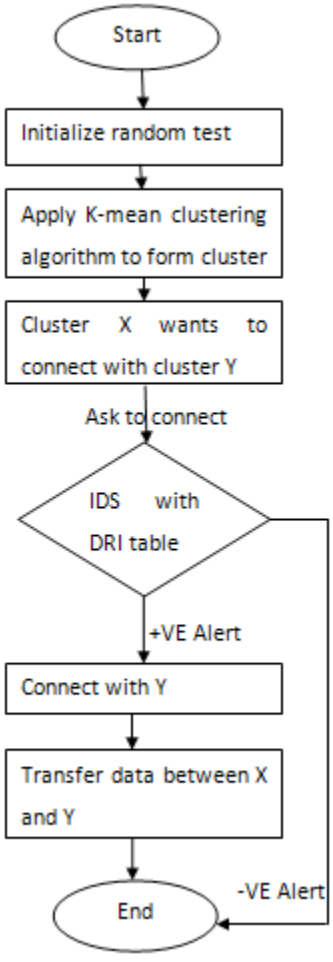

Figure 1. Flow Chart.

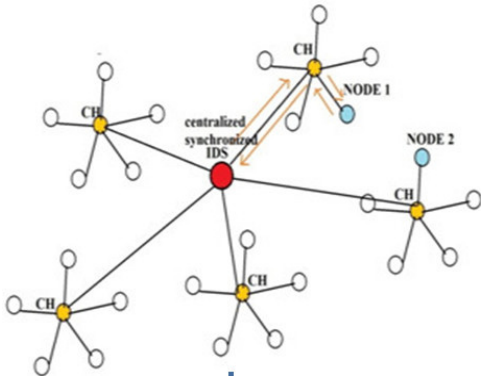

Figure 2. Formation of nodes, centralized IDS and cluster heads.

3. Expected Outcomes

In Black Hole attack or packet drop attack, malicious node drops the received packet and affects the network throughput. The nodes are grouped together to form the clusters and each cluster has a cluster-head. It will collect the all information of every node inside the network and forward to the IDS node. Clustering is used to improve the lifespan of the nodes. When the source node broadcasts to all the neighboring nodes in the cluster, the route request message will be received to all the nodes in the cluster. If a network is under a black hole attack, then the black hole immediately revert with the route reply message having a very smaller delay than the original destination node to the source node. This technique is similar to the functionality of anomaly detection technique.

The proposed work contains the anomaly detection techniques which are based on certain parameter to detect the intrusion properly. The contents of the parameter are DRI (Through From) table, loss rate (mean how many packets were lost per node in previous transmission), Transmission rate (mean how many packet were successfully transmitted), Trust rate (that will provide by neighbor nodes), Packet drop ratio, communication between one node with all other nodes, communication access time, communication delay. By using this parameter the IDS will detect the intrusion. It is expected that the proposed technique will detect intrusion which can effect. It can prevent the intrusion attack also. It will also help to inform the cluster about its nodes that any node is black hole here or not.

Cluster Division:

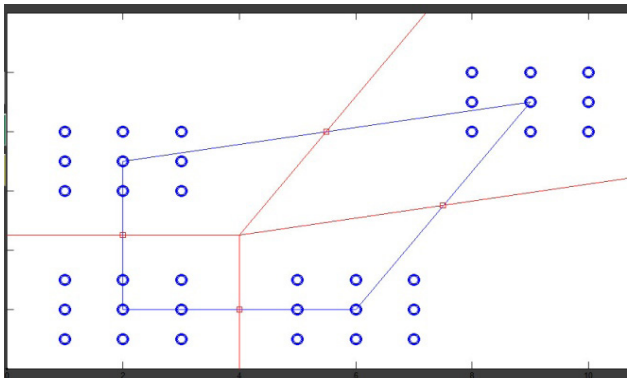

Figure 3. Cluster division.

In this case, random nodes are divides into different clusters. The cluster division is taken place using distance parameter.

3.1 Cluster Head Selection

In this case, Cluster heads will select using distance parameter and energy. Here the node which is shorter distance between all the nodes inside the network, that node will select as a cluster head. After selecting cluster head all cluster head will synchronies with IDS node after deploying IDS inside the network.

Synchronize cluster heads with IDS

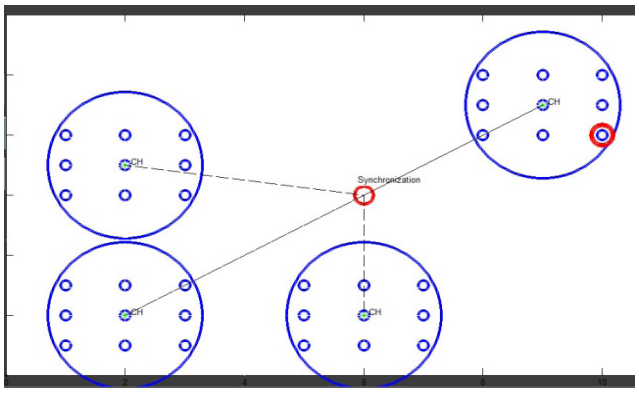

Figure 4. Nodes synchronies with IDS.

Here the cluster heads synchronies information with IDS and will find the malicious node. IDS will get all nodes information from all cluster heads and putting all the data in the data routing table inside the IDS. Message communication takes place from one node to another node inside the cluster with the help of DRI table and from one cluster to another cluster after getting permission from centralized IDS. If node history is suitable in the DRI table then data communication will take place otherwise data communication will be rejected.

3.2 New node inside the Network

First of all the cluster head sends a dummy packet to the new node. If the new nodes wants to communicate with any destination node then IDS checks whether a new node is able to send the packet successfully to the destination node or not. If data sent successfully, it means this new node is not a malicious node, it's a good node and it can use for future communication. In case, data is transmitted from cluster head to cluster head and the new node dropping the packet so it is a malicious node and it's cluster head will inform IDS that this node is a malicious node and it will not able to communication with any other node in future.

4. Conclusion

The proposed technique will helps to prevent the black hole attacks. The synchronized IDS node will work on the base of anomaly detection technique. It will create pattern for malicious activates and detect the intrusion. This technique will helps to enhance security in wireless network and make reliable network for users where the IDS will check all the nodes history to detect the black hole node inside the network. The detection and isolation mechanism for the black hole node in the wireless networks proves to be efficient then the simulation environment without the detection mechanism. However, the proposed detection mechanism is for the single or multiple black hole nodes independent of the other black hole nodes. If there are a huge number of black hole nodes which communicate with themselves, it cannot be detected by the detection mechanism. Hence, the future work can be implementing this detection and isolation mechanism for the huge number of black hole nodes in the wireless networks.

5. References

1. Kao KF, Chen WC, Chang JC, Te Chu H. An Accurate Fake Access Point Detection Method based on Deviation of Beacon Time Interval. 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion (SERE-C), IEEE. 2014 Jun 30. p. 1–2.

2. Kim T, Park H, Jung H, Lee H. Online Detection of Fake Access Points Using Received Signal Strengths. In Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, IEEE. 2012 May 6. p. 1–5.
3. Long X, Sikdar B. A mechanism for detecting session hijacks in wireless networks. IEEE Transactions on Wireless Communications. 2010 Apr; 9(4):1380–9.
4. Marchese M, Surlinelli R, Zappatore S. Monitoring unauthorized internet accesses through a 'honeypot'system. International Journal of Communication Systems. 2011 Jan 1; 24(1):75–93.
5. Nguyen TD, Nguyen DH, Tran BN, Vu H, Mittal N. A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks. 2008. ICCCN'08. Proceedings of 17th International Conference on Computer Communications and Networks, IEEE. 2008 Aug 3. p. 1–6.
6. O'Connor TJ. Detecting and responding to data link layer attacks. SANS Institute InfoSec Reading Room. 2010 Oct; 13.
7. Nikiforakis N, Meert W, Younan Y, Johns M, Joosen W. SessionShield: Lightweight protection against session hijacking. Engineering Secure Software and Systems, Springer Berlin Heidelberg. 2011 Feb 9; 87–100.
8. Luhach Ak, luhach R. Research and implementation of security framework for small and medium sized e-commerce based on SOA. Journal of Theoretical and Applied Information Technology. 2015 Dec 31; 82(3).
9. Dacosta I, Chakradeo S, Ahamad M, Traynor P. One-time cookies: Preventing session hijacking attacks with disposable credentials.
10. Luhach AK, Dwivedi SK, Jha CK. Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA. 2014 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE. 2014 Dec 18. p. 1–6.
11. Dacosta I, Chakradeo S, Ahamad M, Traynor P. One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. ACM Transactions on Internet Technology (TOIT). 2012 Jun 1; 12(1):1.
12. Chomsiri T. A comparative study of security level of Hotmail, Gmail and Yahoo mail by using session hijacking hacking test. IJCSNS. 2008 May; 8(5):23.
13. Luhach AK, Dwivedi SK, Jha CK. Implementing the Logical Security Framework for E-Commerce Based on Service-Oriented Architecture. Proceedings of International Conference on ICT for Sustainable Development, Springer Singapore. 2016. p. 1–13.
14. Prasad SS, Srinath MV, Basha MS. Intrusion Detection Systems, Tools and Techniques–An Overview. Indian Journal of Science and Technology. 2015 Jan 14; 8(35).
15. Amudha P, Karthik S, Sivakumari S. An Experimental Analysis of Hybrid Classification Approach for Intrusion Detection. Indian Journal of Science and Technology. 2016 Apr 18; 9(13).