Access Violation Notification in Wireless Mobile Network Using Entropy Method

L Pushparani, J.Ahalya Mary, S.Sruthi

PG Scholar,CSE Department,SRM University,Chennai

Asst.Professor in CSE Department,SRM University,Chennai

PG Scholar,CSE Department,SRM University,Chennai

***Abstract*—Violation Notification is an important sub task of intrusion detection. Wireless sensor networks are hard to be stable and vulnerable to various attacks. Intrusion alerts are clustered based on the information of mobile terminals. Wireless sensor original notification converted to hyper alerts using clustering method. Intrusion notification clustering method includes notification creation, notification reduction and notification classification. Entropy based trust model in wireless sensor network provides high level of security by path selection based on packet requirement. Entropy trust based model has been interpreted as reputation, trust opinion, probability has been calculated based ob packet re-transmission, packet loss and energy consumption.**

***Index Terms*—mobile Internet; wireless intrusion; notification clustering; network security; entropy method**

I. INTRODUCTION

Original Security Alerts captured by intrusion detection installed in the wireless sensor. Notification creation is an information about access point, mobile terminals mobile terminal types, service set identifier the MAC address, signal strength, whether encrypted or not and database.

Notification reduction is the process of reducing alerts produced by wireless intrusion detection system contains large number of repetitive and unrelated alerts. Unrelated notification like wired equipment privacy is an encryption to secure wireless access point while its encryption.

2. Related Works

Trust has been calculated between different nodes in wireless sensor network that provides stability and security for the nodes that has been described in an entropy based trust modeling and evaluation for wireless sensor network.

Minimal trust routing entropy has avoiding the low trusted nodes in wireless sensor network in the certain part of domain has been described in the secure network admission and routing model based on trust theory using flooding algorithm.

Various severity alerts detected from wireless sensor network has been stored in the log file with various parameters that has been revealed by a detailed analysis of such logs in the form of alert. Different alerts produced by alow level intrusion detection system has been clustered in wireless network, which has been described in Online Intrusion Aggregation with generative data system modeling.

Duplicate alerts or false alerts has been clustered in wireless sensor network using clustering approach in week intrusion detection system. Wireless mesh network which selects node as monitor node periodically based on the timed automate. Monitor node collects the behavior of each node in network including packet transmission, packet loss, packet re-transmission, energy efficiency and detects real time attacks by various device without signature of intrusion or various trained data.

Hybrid Intrusion cluster based detection in wired and wireless network detects the various intrusion based on the components like profiles, subject, activity rules, anomaly records, audit records and objects. This model has been defined as Rule-based pattern matching algorithm intrusion-detection.

Common Intrusion-Detection framework (CIDF) detects the intrusion in wireless network based on components like event generators, response unit, event analyzers and event database. Intrusion Detection Message Exchange Format (IDMEF) share the intrusion detection information in the form of alerts, which provides more interaction between the intrusion detection system and other various security system and express the relationship with the nodes in encryption mechanism of the access point for improving intrusion detection message exchange alert format.

Quantitative alert correlation method uses alert IP address to analyze the relationship between attacks and aggregates the various alerts into high level alerts.

3. Overview of Access Violation Notification

Access violation notification in a wireless sensor network has been clustered and removed unwanted alerts from the clustered alerts. Provide service to a trusted mobile device in wireless network. Trusted device has been identified using entropy method with various parameters. Trust based routing algorithm is implemented to provide high level security for

path selection based on the requirements of trusted packets.

Access Violation Notification framework

Access violation notification has been received from a wireless network and provide service to a trusted mobile device based on trusted established between various different nodes in a network with trusted information.

Creation of wireless nodes in the wireless and gathering the characteristics about the device before creating the node in a wireless sensor network. Type of addressing structure used in the simulation device and define the network components based on tracking device enabled in mobile device.

Wireless notification has been formatting by original security notification captured by Intrusion detection system installed in wireless sensor network. Notification has been captured based on the functionality of mobile device using monitor mode or wireless card installed in mobile. Notification has been formatting based on the information about access point, working channel, mobile terminal types, MAC address, SSID, signal strength and check whether the encrypted or not and access point encryption mechanism.

Notification received from intrusion detection in wireless sensor network has been filtered based on the unwanted notification from the various unwanted device and notification received from the particular device repeatedly with invalid information. When mobile device trying to access the wireless network with invalid information repeatedly, which generates notification from the server side frequently. Service provider filters the unwanted notification and repeated notification by the various mobile node to increase the accuracy and reliability of notification.

Unrelated Notification includes three levels: Data Source, Network Security and result relevance to device.

1. Data Source: Spatial characteristics used to find the type of wireless sensor from formatted notification provided by wireless network identification like Snort Wireless
2. Result Relevant to Node: combined with data source and network details and find type of attack described by notification meets and finally describe result as whether the notification is relevant.
3. Network Environment: Gather information about target device like Access point, MAC address, mobile terminals, SSID and encrypted or not.

$$\text{Filtering Rate} = \frac{\text{N(original)} - \text{N (Filtered)} \times 100\%}{\text{N (original notification)}}$$

1. First define the attack type set A={a1,...ai}, the loophole of wireless device set WD={wd1,...wdi}, and the information of wireless device set Id={id1,...idn};
2) Element has been set in clustering predicate 1, predicate 2 and predicate 3. Every element has a range of {1,0}, while 1 refers TRUE, 0 refers FALSE;
3) Notification relevance function, check whether generated notification and target device are equivalent. Final output to do notification reduction

Entropy-based trust model establish the trust relationship between two nodes in same location or various location. One node trust the other node to perform various actions and exchange the data between two nodes in same or different location. One node is referring as subject and another node refers as agent. Trust interpreted as trust opinion, reputation and probability. Entropy trust model provides more reliability to notification by avoiding packet Re-transmission, packet loss, reputation and energy consumption.

Trust Routing

Trust based routing provides high level of security by path selection in wireless network based on trusted packet in the network. Route has been established between various source to various destination nodes. Most wireless sensor networks application carries and deliver very secret information like military and health applications, this type of secure information has been infected by misbehaving nodes in wireless network misroutes packets to various untrusted destination which leads to loss of information.

Trust Routing protocol protects the data and exchange the data, secure information deliver to trusted destination and protects the confidential information from the untrusted routes. Trust routing provides the good relationship between two different nodes.

Notification Clustering

Service set identifier of access point and MAC address of the various attack source and destination are introduced to classify the notification with various combination like alert type, source MAC, destination MAC and Timestamp.

Type 1: same notification type, source MAC and destination MAC attributes in same class.
Type 2: same notification type and source MAC but different destination MAC attributes in same class.
Type 3: same notification type and destination MAC but different source MAC attributes into a same class.

4. Problem Statement

The access violation notification method reduces a bunch of repetitive and unrelated notification from the original notification, and finally, turns the reduced alerts into the hyper notification.

Access violation notification has been defined in three ways.

- Notification Formation
- Notification Filtering
- Notification Clustering

Original alerts from wireless sensor network has been converted to hyper alert based on source MAC, destination MAC, timestamp and alert Type. Entropy trust model has applied to provide a high level of security by path selection based on packet trust requirement. Entropy based trust model follows actions like reputation, trust opinion, probability.

System Archtecture

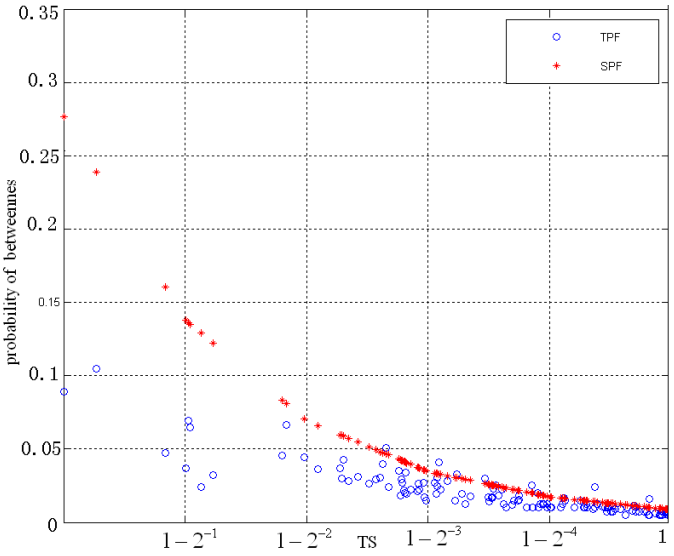
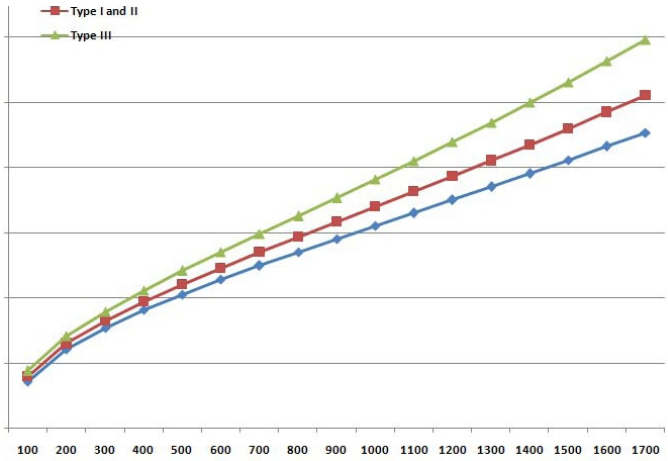


Figure 2 : Comparison between Shortest path and Trust

Trust has been calculated eventually between all the nodes in a wireless network. Calculating Trust between nodes helps to avoid network risk for accessing network by trusted system; Provides more concentrated on the nodes with high TS; nodes with low TS has been decreased obviously.



Entropy-model trustworthiness with the nodes from 100 to 1700, of which 10 percent are malicious nodes.

Entropy based action modelling has calculated the probability P performance as

$$H(X,Y) = - \sum_x \sum_y p(x,y) \log_{2P(x,y)}$$

Average Trusted Entropy

$$H(X) = - \sum_x p(x) \log_{2P(x)}$$
$$= -\sum_x m \log 2m$$
$$= N m \log 2m \qquad m \in [0,1]$$

For wireless sensor network at a moment , p(x) basically accurate with their worthiness Let $P = \sum_x p(x)$which is a fixed value with the current wireless sensor conditions. Considering that the process of entropy calculation and the fact that log1 0, log2 1,

Clustering Algorithm

```
While(i≤j)
{
  If(notification(i).notificationType not belong to HAI)
   {
     If (notification(i).notificationType is a new type ||
     notification(i).sourceMAC and notification(i) .
     destinationMAC are new address)
     {
     add notificationType to cluster notification attack type;
     classify ak to cluster notification indication;
     add sourceMAC and destinationMAC to HAI's SMAC
     and DMAC;
      k++;
      i++;
      }
     elseif (notification (i).sourceMAC and
      notification (i) of  .destestinationMAC are new address)
     {
     classify ak to HAI;
      add sourceMAC and destMAC to cluster
     SMAC and  DMAC;
```

```
  k++;
  i++;
 }
  cluster ak to Cluster notification II;
    k++;
     i++;
  }
 }
 remove Type from attack type and add it to  attack type;
add sourceMAC and destinationMAC to HAIII's
 SMAC and DMAC
```

Various Attacks in Wireless network

1	association request flood	DoS Attack
2	authentication flood	DoS Attack
3	RF jamming attack	DoS Attack
4	NULL probe response	Abnormal Frame
5	malicious AP	Rogue AP
6	unclassified AP	Rogue AP
7	MAC spoofing	MAC Spoofing
8	ARP replay attack	WEP Crack
9	tkiptun attack	WPA Crack
10	reserved management E&F	Abnormal Frame
11	minidwep attack	WPA Crack
12	wellenreiter probing	War Driving
13	netstumbler probing	War Driving
14	airodump probing	War Driving
15	EAPOL flood	DoS Attack

Conclusion

Access violation notification method reduces a bunch of repetitive and unrelated notification from the original notification and finally, turns the reduced notification into the clustered trusted notification. Entropy based trust model has been applied to provide a high level of security by path selection based on packet trust requirement. Entropy based trust model follows actions like reputation, trust opinion, probability. Finally Provide Service and permission to Trusted device to access network.

References

[1] Denning.D, "An intrusion-detection model", IEEE Transactions on Software Engineering, vol.13, no.2, pp 222-232, February, 1987.

[2] Yi Ping, Wu Yue, Liu Ning, Wang Zhiyang, "Intrusion detection for wireless mesh networks using finite state machine", China Communications, vol.7, no.5, pp 40-48, May, 2010.

[3] Mu Chengpo, Huang Houkuan, Tian Shengfeng, "A survey of intrusion-detection alert aggregation and correlation techniques", Journal of Computer Research and Development, vol.31, no.1 pp 1-8, January, 2006.

[4] Patel Ahmed, Qassim Qais, Wills Christopher, "A survey of intrusion detection and prevention systems", Information Management and Computer Security, vol.18, no.4, pp 277-290, September, 2010.

[5] Zhiping Jiang, Jizhong Zhao, Xiang-Yang Li, Jinsong Han, Wei Xi, "Rejecting the attack: source authentication for Wi-Fi management frames using CSI information", In Proceedings of the 32nd IEEE Conference on Computer Communications (INFOCOM 2013), Turin, Italy, pp 2544- 2552, April, 2013.

[6] Valeur Fredrik, Vigna Giovanni, Kruegel Christopher, Richard A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation", IEEE Transactions on Dependable and Secure Computing, vol.1, no.3, pp 146-169, July, 2004.

[7] Zhang S., Ford J., and Makedon F., "Analysis of a low dimensional linear model under recommendation attacks," in Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval, 2006, pp.517-524.

[8] Mingwu, Zhang, Bo, Yang, Yu, Qi and Wenzheng, Zhang, "Using Trust Metric to Detect Malicious Behaviors in WSNs," in Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007, Vol. 3, pp. 104 - 108.

[9] S. Yan Lindsay, Y. Wei, H. Zhu, and K. J. R. A. L. K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 305-317,2006.

[10] K. Romer and F. Mattern, "The design space of wireless sensor networks," Wireless Communications, IEEE [see also IEEE Personal Communications], vol. 11, pp. 54-61, 2004.

[11] B Tadić, S Thurner2, and G. J. Rodgers. "Traffic on complex networks: Towards understanding global statistical properties from microscopic density fluctuations". Phys. Rev. E 69, 036102, 2004.

[12] X.J.Hu, P.D.Zhu, and Z.H.Gong. "Translator Trust for the Internet Inter-domain Routing", IEEE Future Generation Communication and Networking,2007,1,pp.453 – 458

[13] X. Yongxiang, D.J.Hill. "Attack vulnerability of complex communication networks", IEEE transactions on circuits and system. 2008, 55(1),pp.65-68

[14] J.Zhang, H.Y.Hu, and M.Tong. "A Security Metric and Related Security Routing Algorithm Design Based on Trust Model",Journal of Electronics and Information Technology, 2008, 30(1),pp.10-15