International Journal of Research Instinct
(Peer-reviewed Journal)

ISSN ONLINE 2348-2095
Research Article

A Proficient Double-layer Intrusion Recognition exposing in MANET with Voice over IP

[1.] T. Mahalakshmi, [2.] S. Sarugasini
1&2.Asst.Professor., Caussanel College of Arts and Science, Muthupettai.
neveraj2004@gmail.com, charuhasinimca@gmail.com

ABSTRACT

In this hasten humanity, the networks are useful in operating the user's device they are dynamic in nature but at the same time, they are highly vulnerable to attacks. When the user is mobile, the session may not hold good and the communication may get hand-off. The **MANET** comes into depiction when the user is moving. The nodes of the network keep on moving with different speeds, which results in the variations in the structure of the network. This characteristic of the MANET may cause harm within the infrastructure. Intrusion Detection Systems (IDS) provides conflict by contributing support of audit and monitoring at the nodes level. It also responds to these kinds of attacks at the network level. Efficient communication of MANET is critical for the performance of wireless & mobile computing systems. The centralized algorithms proposed in literature are neither robust, nor scalable. In this research we focus the MANET with voice data packets. Mainly this context focuses voice packets used by VoIP. Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. VoIP is available on many smart phones, personal computers, and on Internet access devices. MANET can be classified as clustering of efficient nodes to make an efficient communication. This system proposes double-layer detection method for VoIP IDS in MANET as S**ort slanting and Clustered Multi-level Detection Approach**. Sort slanting detection denotes the functionality of accumulating provision from multiple packets and using the aggregated condition in the rule matching System.

1. INTRODUCTION

Intrusion detection is the process of identifying and/or blocking any attempt to bypass the security of a system. Due to the continuous evolution of Information and Communication Technology (ICT), intrusion detection is an open and volatile research field. Exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage. The complexity of network and information systems increase, so does the capabilities of adversaries, which continuously forces the intrusion detection research to adapt to new adversaries.

Intrusion detection is no longer valid. Moreover, intrusion detection must also face the challenge posed by new paradigms in computing and communications, including cloud computing and the new generation of wireless technologies. This section first reviews the Classification of IDS Then, the main detection approaches are presented, with special emphasis which have been widely used for anomaly detection and are subject of study in parts of this Paper. Finally, we discuss the need of IDS's to address the deficiencies of classical IDSs.

2. OBJECTIVE

In the MANET, there would be various kinds of intrusions which occur during the transactions such as backdoor, email spoofing, etc. Protecting your network from intruders and attackers is to be effective, network security should be multilayered. You would protect your home from burglars by installing fencing at the property line (perimeter), putting locks on the doors and windows, installing a motion detector inside the house, and finally putting very valuable items in a safe concealed in the wall. Likewise, your network needs its own levels of protection: perimeter protection (a firewall) at the point it connects to the Internet, access controls (user accounts and permissions) to restrict access to data if someone does get into the network, and encryption of particularly sensitive data.

The main objective of this research, the intrusion detection is handled with an innovative technique to secure transmission for the VoIP data transmission. In addition, to these the intrusion detection is undertaken within a single framework authentication. This context is mainly focuses on the double-layer detection for the internet users transmitting information within the networks wherever in the world should be secure. It is the first line of defense against malware. There is sometimes confusion between an IPS and a firewall. Personal firewalls are more basic, making allow/deny decisions to ensure that only “selected” programs are allowed to interact over the internet. Firewalls also block network communication on non-standard ports, which are generally not used by legitimate programs and services. On the other hand, an IPS goes one step further, and examines all network traffic that is allowed through the firewall. In order to avoid the performance degrading of the networks, the IPS must efforts as a proficient security component. Prevention system occupies quick because utilizes can happen. The prevention system would recognize and act in response exactly to avoid the intrusions.

The key challenge in the MANET is the way bandwidth is allotted capably to introduce quality of service. This paper proposes a novel technique to make efficient security feature to the routing during transmission within the network. The key challenge is to prevent the intrusion which would affect the transmitted data. In the earlier sections, the information would be transmitted over the network with security constraints like encryption, digital-signature, providing keys, etc. There are several encryption algorithm are presented to encrypt the transmitted data. The innovative technique to make detection of the intrusions within this wireless networks is endorsed in the form of layer-layer architecture.

3. MANET VULNERABILITIES

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user’s identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

1. Lack of centralized management:

MANET doesn’t have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

2. Resource availability:

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3. Scalability:

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4. Cooperativeness:

Routing algorithm for MANETs usually assumesthatnodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

5. Dynamic topology:

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

6. Limited power supply:

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

7. Bandwidth constraint**:**

Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

8. Adversary inside the Network:

The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

9. No predefined Boundary:

In mobile ad-hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [2].

4. SECURITY GOALS:

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1. Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

2. Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

3. Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

4. Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators.

5. MANET CHARACTERISTICS:

1) Distributed operation: There is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

2) Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

4) Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

5) Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

6) Shared Physical Medium**:** The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

6. METHODOLOGY

The wireless network transactions faces an range of intimidation that take benefits of numerous vulnerabilities commonly found Thus, the stipulation of protection in the network indeed. Also in the allocation of bandwidth during the communication may cause defense issues in such devices. The key dispute of this context is to focus on the dilemma of Intrusion in the networks to make a secure announcement within MANET with VoIP. The key challenge is to make protected transactions of the networks by preventing the intrusion occurs during transmission using clustering technique. The bandwidth allotment is the major issue in the MANET to communicate with the member nodes within the networks. Because, whenever a source wants to make a communication with a destination, it must submit a request for a routing to a node. The probability of the communication to be dropped or blocking originated in the networks can be minimized. The dropped or blocking probability can be avoided by increasing the channels, but the networks have a limited frequency to allocate for the communication and there is a limit to maximize the number of channels. The probability of dropped or blocking of the communication is arises because of the ingression of the *intruder* within that routing. Before that know about how the Intrusions enters into the networks. Intrusions are the activities that violate the security policy of system. Intrusion Detection (ID) is the process used to identify intrusions. The intrusion detection may classify as Host-based intrusion, Distributed intrusion and Network-based intrusion. The host-based ID detects attacks against a single host. The distributed ID detects attacks involving multiple hosts. The network-based ID detects attacks from networks.

This paper is to motivate that the intrusion transpire within the networks would degrade the recital of the networks. Due to the openness of the wireless networks the nodes may meandering anywhere within the networks, this kind of networks may countenance various attack vulnerabilities. These vulnerable attacks appear into the networks without any familiarity of the network members. Thus there would be a need for an intrusion detection and prevention system. A novel technique discovered in this thesis was exertion as a detection system, clustering technique is involved to reduce the route discovery & false alarms and innovative encryption techniques were included with the traditional intrusion detection system to allocate the secure bandwidth for voice data packets within the wireless networks. Intruders might be starting external network or valid users of the network. Intrude arises in different way within the networks like unexpected combinations, unhandled input, buffer overflows, etc. Intrusion detection on the network is an intense explore field in communication, where much work has been done during the past two decades. Several business firms construct a network-based intrusion detection system, an existing device learning algorithm. The research describes that the existing system could achieve a low down fake positive rate while keeping a preferable detection of intrusion but the transmitted data would be interrupted before the intrusion is detected.

7. MANET APPLICATIONS:

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include [12, 16]

1. Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

2. Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3. Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

4. Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

5. MANET-VoVoN**:** A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels [17].

8. CONCLUSION:

In this paper, we have presented and discussed the taxonomy of routing protocols in mobile ad hoc networks and provided comparisons between them. The protocols are divided into three main categories: (i) source-initiated (reactive or on-demand), (ii) table-driven (pro-active), (iii) hybrid protocols. For each of these classes, we reviewed and compared several representative protocols. While there are still many challenges facing Mobile ad hoc networks related to routing and security. Each routing protocol has unique features. Based on network environments, we have to choose the suitable routing protocol. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The main differentiating factor between the protocols is the ways of finding and maintaining the routes between source destination pairs. The comparison we have presented between the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. We hope that the taxonomy presented in this paper will be helpful and provide researchers a platform for choosing the right protocol for their work. At last we have provided the overall characteristic features of all routing protocols and described which protocols may perform best in large networks. Almost all the protocols we discussed in this paper have their own characteristic features and performance parameter combinations where they out perform their competitors. Still mobile ad hoc networks have posed a great challenge for the researchers due to changing topology and security attacks, and none of the protocols is fully secured and research is going on around the globe.

9. FUTURE WORK:

Routing protocol DSDV uses proactive “table driven” routing, while AODV and DSR use reactive “on-demand” routing. Protocol DSDV periodically updates its routing tables, even in cases when network topology doesn’t change. AODV protocol has inefficient route maintenance, because it has to initiate a route discovery process every time network topology changes. Both protocols, AODV and DSR, use route discovery process, but with different routing mechanisms. In particular, AODV uses routing tables, one route per destination, and destination sequence numbers as a mechanism for determining freshness of routes and route loops prevention. On the other hand, DSR uses source routing and route caching, and doesn’t depend on any periodic or time-based operations. Generally, we can conclude that in low mobility and low load scenarios, all three protocols react in a similar way, while with mobility or load increasing DSR outperforms AODV and DSDV routing protocols. Poor performances of DSR routing protocol, when mobility or load are increased, are the consequence of aggressive use of caching and lack of any mechanism to expire stale routes or determine the freshness of routes when multiple choices are available. However, there are many other challenges to be faced in routing protocols design. A central challenge is the development of the dynamic routing protocol that can efficiently find routes between two communication nodes. Also, in order to analyze and improve existing or new MANET routing protocols, it is desirable to examine other metrics like power consumption, fault tolerance, number of hops, jitter, etc. in various mobility and traffic models.

REFERENCES

[1] Tiranuch Anantvalee, Jie Wu, “A Survey of Intrusion Detection in Mobile Ad Hoc Networks”, Wireless/Mobile Network Security, 2006 Springer.

[2] Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris, “Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms”

[3] Yi-an Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”

[4] Ehsan Amiria, Hassan Keshavarzb, Hossein Heidaria, Esmaeil Mohamadic, Hossein Moradzadeh, “Intrusion Detection Systems in MANET: A Review”, International Conference on Innovation, Management and Technology Research, 2014

[5] Aikaterini Mitrokotsaa, Christos Dimitrakakis, “Intrusion detection in MANET using classification algorithms: The effects of cost and model selection”, Science Direct, 2013

[6] Said El brak, Mohammed Bouhorma, Anouar A.Boudhir, “voip over MANET (voman): qos & Performance Analysis of Routing Protocols for Different Audio Codecs”, International Journal of Computer Applications, 2011

[7] S. El Brak,M. Bouhorma,M. El Brak,A.A. Boudhir, “Voip Applications Over Manet: Codec Performance Enhancement By Tuning Routing Protocol Parameters”, Journal of Theoretical and Applied Information Technology, 2013

[8] Yi Sun ,Gengfa Fang, Jinglin Shi, “Research on the Implementation of voip Service in Mobile Ad-hoc Network”

[9] Jen-Jee Chen, Yu-Li Cheng, Yu-Chee Tseng, and Quincy Wu, “A Push-Based voip Service for an Internet-Enabled Mobile Ad Hoc Network”

[10] HuiYao Zhang , Marek E. Bialkowski , Garry A. Einicke , and John Homer, “An Extended AODV Protocol for VoIP Application in Mobile Ad Hoc Network”

[11]. Priyanka Goyal, Vinti Parmar and Rahul Rishi, *“MANET: Vulnerabilities, Challenges, Attacks, Application”,* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[12]. Gagandeep, Aashima and Pawan Kumar “*Analysis of Different Security Attacks in MANETs on Protocol*

Stack". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012

[13]. Mohammad Wazid **,** Rajesh Kumar Singh and R. H. Goudar, *"A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques* **"** International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[14]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011

[15] Sunil Taneja and Ashwani Kush, " *A Survey of Routing Protocols in Mobile Ad-Hoc Networks*", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[16] Gary Breed Editorial Director, "*Wireless Ad-Hoc Networks: Basic Concepts*", High Frequency Electronics, March 2007.

[17] Hongmei Deng, Wei Li, and Dharma P. Agrawal, *"Routing Security in Wireless Ad Hoc Networks"* IEEE Communications Magazine • October 2002