INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A NOVEL ENHANCED INTRUSION DETECTION SCHEME FOR MANET

Nithya[1], Sivakumar[2]

[1] *Research Scholar, Department of Computer Science, PGP College of Arts and Science, Nammakkal, Tamilnadu, ms.nithi04@gmail.com*

[2] *Assistant Professor, Department of Computer Science, PGP College of Arts and Science, Nammakkal, Tamilnadu, ssk.pgp@gmail.com*

Abstract

In the recent decades the mobile wireless communication becomes more attractive because of its applications in many fields. Moving from the wired communication to wireless communication, the security is the most important property to consider. Specifically in the mobile environment it has the vulnerability, because of its portability and scalability. The mobile ad hoc wireless communication has characteristics such as open medium, distributed environment and changing topology, it makes the network into most vulnerable to the attackers to make the intrusion. The attackers (intruders) can easily enter into the network and compromises the network to behave in the favours of his choice. The Mobile Ad hoc NETwork (MANET) should have the capability to detect such intrusion (attacks) and remove it. To survive the MANET from such intrusion, an Intrusion Detection System (IDS) should be enhanced to the MANET, which can efficiently identify the attacks of the intruders. In this paper it is discussed about various intrusion detection mechanisms and techniques for the MANET to detect the intrusion and intruders.

Keywords*:* Intrusion detection system, MANET, Digital Signature algorithm

1. Introduction

The set of actions that compromises confidentiality, availability, and integrity of a mobile node is called as Intrusion [1]. Someone who involved with the compromising networks and performs the intrusion is called intruder. The IDS can monitor the host computer, network equipment, a firewall, a router, a corporate network, or any information system. To detect the presence of intrusion in the network the intrusion detection system (IDS) is used. It is the kind of security technology that attempts to identify, those misbehaving actions of a network and those who have legitimate access to the system but are abusing their privileges [2]. The IDS inspects the network activity, identifies suspicious patterns and indicates the network attack, from someone attempting to break the network.

The IDS should dynamically monitor the network and user's actions in the network to detect intrusions. The network can suffer from various kinds of security vulnerabilities and attackers. It may cause both technically difficult and economically costly to build and maintain a network that is not susceptible to attacks in the mobile environment [3]. An IDS, by analyzing the system and users' operations, in search of

undesirable and suspicious activities, may effectively monitor and protect against threats.

Generally, there are three types of intrusion detection methods such as misuse based detection, anomaly based detection and specification based detection [4]. The misuse based detection technique keeps the record on known attack signatures and system vulnerabilities and stores them in a large database for the analysis of the intrusion activities. If the IDS, find a match between current activities and signatures about the attacks that is already documented, an alarm is generated to indicate suspicious activity [5].

An anomaly based detection technique creates the profiles of system states or user behaviours and compares them with current activities of the user or the system. The profile of the system state includes state of the network's traffic load, breakdown, protocol, typical packet size, usage frequency of commands and CPU usage for programs. It also monitors the network segments to compare their states and look for anomalies. If a sufficient deviation is observed, the IDS raise an alarm about the intruders [6]. Anomaly detection can also capable of detecting the unknown attacks. For the detection of novel attacks the misuse detection technique is not as effective, it is because of the lack of corresponding signatures of attacks in network.

Specification based detection evaluates a set of constraints that describe the correct operation of a program or protocol in the network, and monitors the execution of the program with respect to the defined constraints. This detection technique provides the capability to detect previously unknown attacks, with the low false positive alarm rate. However, normal profile of system state is very difficult to build. In a MANET, mobility induced dynamics make it as the challenging task to differentiate the normality and anomaly [4]. It is more challenging to distinguish between false alarms and real intrusions.

An IDS can also be categorized as network-based IDS and host based IDS in the network based IDS, the individual packets flowing in the entire network is analyzed. It detects malicious packets by overlooking the firewall's filtering rules. In a host based system, the IDS examine the intrusion activity by traffic analysis on each individual mobile host. An IDS differs from firewall it only looks for intrusions in the network in order to stop them from happening [6]. The firewall limits the access between networks and does not alert about an attack from inside the network. But IDS evaluates a suspected intrusion, which is taken place in the network and alerts a signal on intrusion. It also overlooks for attacks that originate within a system.

In the following sections it is devoted about the different types of attacks in the MANET and various intrusion detection technologies applied for the MANETs to detect the existence of the intrusion or the intruders in network. Many researchers are devoted several intrusion detection system techniques that are suitable for the MANET.

2. Intrusion Detection in Mobile Ad Hoc Networks

Intrusion detection for the MANETs is a complex, even difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points [15]. Conventional IDS are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This section outlines the issues of intrusion detection for MANETs and reviews the main solutions proposed by the researchers.

For the mobile ad hoc networks, IDS provide solutions that should be self-organized, collaborative and without centralized entity. Most of the MANET routing protocols have some limitations such that, nodes in network assumes all other nodes always cooperate with each other to relay data. This will cause the vulnerability to the attackers with the opportunities to do some intrusion or unwanted activities and also leave one or two compromised nodes. To address these problems, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter into the network, it will be able to completely eliminate the potential damages caused by compromised nodes at the first time of the attack itself. An IDS act as the second layer for MANET and enables the overall security to the MANET.

A. Mishra et al (2004)., proposed [16] different intrusion detection schemes against attacks. Intrusion detection can be defined as the automated detection and subsequent generation of an alarm to alert the security apparatus at a location if intrusions have taken place or are taking place. An IDS is a defence system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security. IDSs achieve detection by continuously monitoring the network for unusual activity. The

prevention part may involve issuing alerts as well as taking direct preventive measures such as blocking a suspected connection. In other words, intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the network and external ones. Unlike firewalls which are the first line of defence, IDSs come into the picture only after an intrusion has occurred and a node or network has been compromised. That is why IDSs are aptly called the second line of defence.

3. Intrusion Detection Techniques for Mobile Ad Hoc Networks

Many researches are devoted their work for improving and developing the intrusion detection technologies for the MANET [1], [18]-[21]. In line these developments the different type ids for MANET such as watchdog algorithm, TWOACK algorithm, AACK scheme, Digital Signature Algorithm are explained in this section.

3.1 Watchdog algorithm

Marti et al., (2000) proposed [17] a scheme named Watchdog algorithm aims to improve the throughput of network with the presence of malicious nodes in the network. In fact, the Watchdog scheme is consisted of two parts: Watchdog and Path rater. Watchdog serves as the IDS for MANETs. Watchdog node is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listening to its next hop's transmission in the entire network. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time then, it increases its failure counter.

Whenever a node's failure counter exceeds a predefined threshold value, Watchdog node reports it as the misbehaving node. However, compared to some other schemes, Watchdog algorithm is capable of detecting malicious nodes rather than links. Many MANET IDSs are developed as an improvement to the Watchdog algorithm. The Watchdog scheme fails to detect malicious misbehaviours with the presence of the following: ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour report, collusion, partial dropping.

3.2 TWOACK Scheme

TWOACK algorithm was proposed [18] by Liu et al., (2007) is one of the most important approach in which the weaknesses of the Watchdog algorithm were to be solved. TWOACK is neither an enhancement nor a Watchdog based scheme. TWOACK algorithm is aiming to resolve the receiver collision and limited transmission power problems of Watchdog scheme. The TWOACK scheme detects misbehaving nodes by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination in network. It means that, each node required to send back an acknowledgment packet to the node that is two nodes away from it by using the same route.

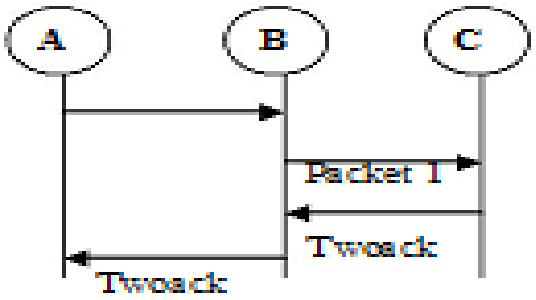

Fig 1: TWOACK scheme

TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) and on-demand routing protocols. The working process of TWOACK algorithm is shown in Fig. 1. In the Fig. 1, the Node A first forwards the Packet 1 to node B then, node B forwards it to node C.

When the node C receives Packet 1, as it is two hops away from the node A, node C is obliged to

generate a TWOACK packet. The TWOACK packet contains the reverse route from the node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from the node A to node C is successful. If the TWOACK packet is not received in a predefined time period, both nodes B and C are reported as malicious nodes. The same process applies to every three consecutive nodes along the rest of the route in the whole network. The TWOACK algorithm successfully solves the limited transmission, receiver collision and power problems of the Watchdog scheme. In TWOACK scheme, the acknowledgment process required in every packet transmission, this adds a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, this redundant transmission process can easily degrade the life span of the whole network.

3.3 AACK algorithm

Sheltami et al., (2009) proposed [19] a new scheme called AACK and this algorithm is based on the TWOACK. Similar to TWOACK, AACK scheme also an acknowledgment-based algorithm. It can be considered as a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, the AACK algorithm significantly reduces network overhead while still capable of maintaining and even surpassing the same network throughput in packet transmission. The end-to-end acknowledgment scheme is shown in Fig. 2.

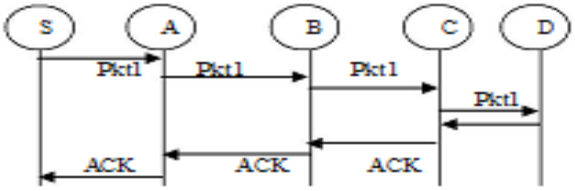

Fig 2: AACK scheme

In the ACK scheme shown in Fig. 2, the source node S first sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet to the neighbour nodes. When the destination node D receives Packet 1, it is required to send back an ACK packet to the source node S along the reverse order of the same route in the network. Within a predefined time period, if the source node S receives this ACK packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out a TWOACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. But both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes in the network with the presence of false misbehaviour report and forged acknowledgment packets.

3.4 The Digital Signature Algorithm (DSA)

The Digital signature algorithm (DSA) has been suggested and standardized by the national institute of standards and technology (NIST) of the U.S[5],[17]. It is an efficient variant of the ElGammal signature scheme [3]. The ElGammal signature scheme has several drawbacks which the DSA repairs.

- Given today security standards, an ElGammal Signature is of bit length at least 2048. A DSA signature is of bit length 320.
- Signature verification in the ElGammal signature requires three modular exponentiations with exponents of bit length at least 1024. Signature verification in the DSA requires only two modular exponentiations with exponents of bit length 160.

The idea for the reduction of the exponent size is taken a signature scheme of schnorr[12] which is patented. There is a discussion whether the schnorr patent covers the DSA.

Step 1: Global Public-Key Components

p prime number where $2^{L1} < p < 2^{L}$ for $512 \leq L \leq 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p\ 1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

$g = h^{(p1)/q} \bmod p$, where h is any integer with $1 < h < (p\ 1)$ such that $h^{(p1)/q} \bmod p > 1$

Step 2: User's Private Key

x random or pseudorandom integer with $0 < x < q$

Step 3: User's Public Key

$y = g^x \bmod p$

Step 4: User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Step 5: Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (H(M) + xr)] \bmod q$

Signature = (r, s)

Step 6: Verifying

$w = (s')^{-1} \bmod q$

$u1 = [H(M')w] \bmod q$

$u2 = (r')w \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

Step 7: TEST: $v = r'$

M = message to be signed

H(M) = hash of M using SHA-1
M', r', s' = received versions of M, r, s

With these numbers in hand, each user selects a private key and generates a public key. The private key x must be a number from 1 to (q1) and should be chosen randomly or pseudo randomly. The public key is calculated from the private key as $y = g^x \bmod p$. The calculation of y given x is relatively straightforward. However, given the public key y, it is believed to be computationally infeasible to determine x, which is the discrete logarithm of y to the base g, mod p.

To create a signature, a user calculates two quantities, r and s, that are functions of the public key components (p, q, g), the user's private key (x), the hash code of the message, H(M), and an additional integer k that should be generated randomly or pseudo randomly and be unique for each signing. The receiver generates a quantity v that is a function of the public key components, the sender's public key, and the hash code of the incoming message. If this quantity matches the r component of the signature, then the signature is validated.

4. Conclusion and Future Work

MANETs are a new technology used increasingly in many applications. Because of the characteristics of the MANET, these networks are more vulnerable to attacks and have most security problems than other networks. In terms of MANET security the Intrusion Detection is the most considerable one. If the IDS are well designed, it can effectively identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defence in depth security mechanisms for MANETs. In this paper, it is briefly explained on existing intrusion detection techniques in the context of MANETs. Since Intrusion prevention alone is not sufficient to achieve security in a network, it is presented a way to manage

MANET security, by enhancing the existing secure protocols adding the component of Malicious nodes, not only in determining the route for sending packets, but also avoiding attempts of Denial of Service from Malicious Nodes. The accuracy of IDS can suffer from the high false positive or low false negative rates. If the majority of the mobile nodes are compromised then the intrusion detection becomes fail. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, which may be addressed in future. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. As a consequence intrusion detection for MANETs remains a complex and challenging topic for security researchers.

5. REFERENCES

[1] B. Sun, L. Osborne, Y. Xiao and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Communications*, pp. 56-63, October 2007.

[2] S. Sen and J. A. Clark, "Intrusion Detection in MANETs," *Department of Computer Science, University of York, York, UK.*

[3] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," *IEEE Wireless Communications*, pp. 48-60, February 2004.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, *Springer*, pp. 170–196, 2006.

[5] J. Zhang and M. Zulkernine, "A Hybrid Network Intrusion Detection Technique Using Random Forests," *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society*, 2006.

[6] C. Xenakis, C. Panos and I. Stavrakakis, "A comparative Evaluation of Intrusion Detection Architectures for MANETs," *computers & security 30, Elsevier*, pp. 63-80, 2011.

[7] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", *IEEE Communications Surveys & Tutorials*, 2013.

[8] M. Bishop, "Computer Security: Art and Science", *Addison Wesley*, Nov. 2002.

[9] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFI-DANT Protocol", *Proc. of ACM Int. Sym. on MANET and Computing*, 2002.

[11] M. Y. Su, "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems," *Computer Communications, Elsevier*, 34, pp.107–117, 2011.

[12] X. Y. Zhang, Y. Sekiya and Y. Wakahara, "Proposal of a Method to Detect Black Hole Attack in MANETs", *Proc. IEEE Inter. Symp. On Autonomous Decentralized System ISADS*, 2009.

[13] E. A. Panaousis, L. Nazaryan and C. Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Sep. 7-9, 2009, London, UK.

[14] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in MANET", *Elsevier*, Ad Hoc Networks, 2008.

[15] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, "Threshold-based Intrusion Detection in Ad Hoc Networks and Secure AODV," *Ad Hoc Networks 6, Elsevier*, pp. 578–599, 2008.

[16] A. Mishra, K. Nadkarni, A. Patcha and V. Techintrusion, "Detection In Wireless Ad Hoc Networks," *IEEE Wireless Communications*, pp. 48-60, February 2004.

[17] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA*, pp. 255–265, 2000.

[18] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[19] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in

presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst., vol. 15, no. 5*, pp. 273–282, Oct. 2009.

[20] J. Cho, I. Chen and P. Feng, "Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks," *IEEE Transactions on Reliability, Vol. 59, No. 1*, pp. 231-241, March 2010.