RESEARCHERID
THOMSON REUTERS

[Preet* *et al.*, 6(5): May, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DESIGNING SECURE MULTICASTING ROUTING ALGORITHMS IN MANET USING IDS

Mrs Pooja Preet*, Dr. Rahul Mishra, Dr. Saket Agrawal

[*] Ph.D.Scholar,Department of Computer Application, IFTM University, Moradabad
Professor,Department of Computer Application, IFTM University, Moradabad
Professor, Rajshree Institute of Management & Technology, Bareilly

DOI: 10.5281/zenodo.573517

ABSTRACT

Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly.This paper aims to pioneer and to assort current techniques of Intrusion Detection System (IDS) aware MANET. MANET is infrastructure-less, pervasive in nature with multi-hop routing, without any centralized authority. To support these ideas, a discussion regarding attacks and researches achievement on MANET are presented inclusively in this paper, and then the comparison among several researches achievement is evaluated based on these parameter.

KEYWORDS: MANET, types of MANET and IDS.

INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links.

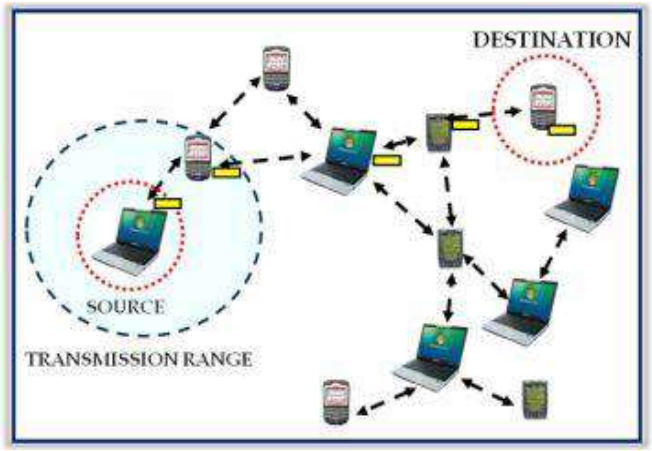

Fig 1: MANET Architecture

This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self-maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances. MANETs are an appealing technology for many applications such as rescue and tactical operations due to the flexibility provided by their infrastructure.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used are ineffective and inefficient for the highly dynamic and resource constrained environments where MANETs use might be expected. Unfortunately, the remote distribution and open medium of MANET makes them susceptible to various attacks. For example, due to lack of protection for nodes, malicious attackers can easily capture and compromise the mobile nodes to achieve attacks. Particularly, considering the fact – that most routing protocols in MANETs assume that every node in the network behave cooperatively with other nodes and presumably not a malicious one attackers can easily compromise MANETs by inserting malicious or non-cooperative node into the network. Due to MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. Hence, it is crucial to develop an intrusion detection system in MANETs. In this synopsis, we aim to develop such an efficient and reliable intrusion detection system (IDS).

CHARACTERISTICS

The characteristics of MANET are identified as follows:

- **Autonomous terminal:** Each node in MANET is autonomous and acts both, as router and host.
- **Distributed:** MANET is distributed in its operation and functionalities, such as routing, host configuration and security.
- **Multi-hop routing:** If the source and destination of a message is out of the range of one node, a multi-hop routing is created.
- **Dynamic network topology:** Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.
- **Fluctuating link bandwidth:** The stability, capacity and reliability of a wireless link are always inferior to wired links.
- **Thin terminal:** The mobile nodes are often light weight, with less powerful CPU, memory and power.

INTRUSION DETECTION SYSTEM (IDS)

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. Depending on the detection techniques used, IDS can be classified into three main categories as follows:

- Signature or misuse based IDS
- Anomaly based IDS
- Specification based IDS

• ***The signature-based IDS*** uses pre-known attack scenarios and compare them with incoming packets traffic. There are several approaches in the signature detection, which differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system, pattern recognition, coloured petri nets , and state transition analysis are grouped on the misuse.

• ***The anomaly-based IDS*** attempts to detect activities that differ from the normal expected system behaviour. This detection has several techniques, i.e.: statistics, neural networks, and other techniques such as immunology, data mining, and Chi-square test utilization. Moreover, a good taxonomy of wired IDS‟s was presented by Debar.
• ***The specification-based*** IDS are hybrid of both the signature and the anomaly based IDS. It monitors the current behaviour of systems according to specifications that describe desired functionality for security-critical entities [48]. A mismatch between current behaviour and the specifications will be reported as an attack.

- MANET does not have any fixed topologies. So the mobile nodes can move freely around the network.
- The MANET can be divided into a SINGLE-HOP and MULTI-HOP networks.
- In single-hop networks the nodes are within communication range can communicate directly with each other.
- Whereas in Multi-hop networks, if the nodes are out of communicating range, the nodes must rely on intermediate nodes to forward the data packets to their destination.
- However, in both type of networks there is no dedicated link available like the links in wired networks.
- The absence of fixed and dedicated link among the nodes leads to severe security threats to the network.
- So an effective Intrusion Detection Scheme (IDS) is needed to safeguard the network from these threats.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

There are several IDS techniques proposed to ensure the secure communication of data packets in the network. They are:-

- Watchdog
- TWO ACK
- AACK

Watchdog: Marti et al. [1] proposed two techniques (Watchdog and Pathrater) that improve the network throughput with the existence of selfish or misbehaving nodes. Consist of two techniques Watchdog and Pathrater. Watchdog serves as IDS and Pathrater cooperates with routing protocols. It detects malicious nodes by overhearing next hop's transmission. A failure counter is occur if the next node fails to forward the data packet. When it exceeds a predefined threshold the node said or marked it is malicious node. The drawback of watchdog are:

- Ambiguous collisions,
- Receiver collisions
- Limited transmission power,
- Falsemisbehaviour report,
- Collusion,
- Partial dropping.

TWOACK: It solves the problem of receiver collision and power limitation of watchdog. In this scheme an acknowledgment of every data packets over every there nodes along transmission path. If ACK is not received within predefined time, the other nodes are marked malicious. TWOACK works on routing protocols such as Dynamic Source Routing (DSR). The disadvantages are:

- Limited battery power
- Network overhead.

AACK: It solves the two problems of watchdog and improves the performance of TWOACK by reducing the routing overhead while maintaining better performance [2]. AACK is a combination of TACK and ACK. It reduces network overhead but fails to detect malicious nodes with false misbehavior report.

MOBILE AD HOC NETWORK CHALLENGES FOR STANDARD IDS

Currently, there are many available IDS; however those IDS (even host-based or network-based) are not suitable for MANET due to the following reasons:

- The nodes may not have enough capabilities to execute the IDS in a continuous manner, due to limited or exhausted resources.
- The hosts are more vulnerable to get captured, compromised, or disconnected.
- There may not be a clear separation between normal and abnormal situations in a mobile environment; thus it is increasingly difficult to distinguish false alarms from real intrusions. It is difficult to obtain enough audit data to make an intrusion detection decision because the bandwidth of MANET is more restricted compared with wired networks. As a result, IDS can either have too many false alarms or miss too many legitimate attacks.
- Nodes may behave maliciously only intermittently, further complicating their detection.
- A node that sends out false routing information may be a compromised node or merely a node that has a temporarily stale routing
- Compared with wired networks, where traffic monitoring is usually done at switches, routers and gateways, the mobile IDS must work with localized and partial data because the ad hoc environment does not have traffic concentration points where the IDS can collect audit data for the entire network.
- Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Under these constraints, the IDS for MANET has been proposed to work in a collaborative way and as part of the existing routing protocols.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

PROPOSED SYSTEM

Here we propose a strong new Intrusion detection mechanism called EAACK which requires less hardware cost. EAACK is an acknowledgement based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets.

- EAACK is divided into three major parts called:
  - ACK
  - S-ACK
  - MRA
- ACK is an end-to-end acknowledgment scheme. EAACK, aiming to reduce low network overhead when no network misbehaviour is detected. To preserve the lifecycle of battery and have low memory consumption.
- According to this ACK mode, if the receiver node does not send the ACK within predefined time interval, then ACK assumes malicious may present and switch to S-ACK mode to detect them.
- In S-ACK part, for every three consecutive nodes in the route, the third node sends an S-ACK acknowledgment packet to the first node. If malicious found, then MRA mode select alternate path to the destination.
- To initiate the MRA mode, the source nodes first searches its local knowledge base and take an alternative route to the destination node.
- If there is no other that exists, the source node starts a routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

REFERENCES

[1] Tiranuch Anantvalee, Jie Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks” Wireless/Mobile Network Security Journal, pp. 170 – 196, 2006 Springer.
[2] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.
[3] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.
[4] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Informatio n Systems (WIS-2002), pp. 1-12, April 2002.
[5] Kachirski and R. Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p.57.1, January 2003.
[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,"Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.
[7] S. Buchegger and J. Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, June 2002.
[8] P. Michiardi and R. Molva, \Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Communication and Multimedia Security Conference (CMS'02), September 2002.
[9] D. B. Johnson, and D. A. Maltz, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft)," Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.
[10] P. Brutch and C. Ko, “Challenges in Intrusion Detection for Wireless Ad-hoc Networks," Proceedings of 2003Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

CITE AN ARTICLE

Preet, P., Mrs, Mishra, R., Dr, & Agrawal, S., Dr. (2017). DESIGNING SECURE MULTICASTING ROUTING ALGORITHMS IN MANET USING IDS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, 6(5), 402-406. doi:10.5281/zenodo.573517

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7