A STUDY ON MANET INTRUSION DETECTION SYSTEMS

Pamidi Naga venkata Siva kumar¹, Nagendra Babu Rajaboina², Pappula sarala³
¹Assistant Professor, ECE department, Vijaya institute of technology for women, sivakumar.pamidi@gmail.com
²Assistant Professor, CSE department, Vijaya institute of technology for women, nagendrarajaboina@gmail.com
³Assistant professor, CSE department, Vijaya institute of technology for women, pappulasarala@gmail.com

ABSTRACT

MANETs consist of certain mobile wireless nodes with limitations such as remaining energy, lifetime of network, stability, etc. Protection is the major weakness in MANET due to the versatility of nodes and constantly shifting dynamic topology, which is very vulnerable to a range of attacks such as eavesdropping, routing, modification of packets. Because of its characteristics such as mobile design, wireless networking connections and the lack of practical hierarchy, MANET suffers from protection problems, deteriorating QoS. It was not necessary to apply the protection solutions offered for any fixed wired network to the mobile wireless network. Thus, intrusion monitoring that controls the device to identify any breach weakness is the better way to ensure protection for MANET. Detecting intrusions plays an essential role in providing protections and serves as an external layer of defenses against unwanted entry.

Keywords: MANET, intrusion, attacks, QoS, blackhole attack

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) relates to one form of mobile network that comprises mobile wireless networking nodes. In random and unpredictable topologies, these nodes arrange themselves dynamically. In such a situation, considering the versatility of the nodes in mind, a wireless device that can deliver knowledge from a source to a destination is critical. This is since, within its frequency spectrum, a node will receive a packet of data that is sent. So, since the nodes are mobile, at any moment, the receiving node will switch out of the frequency range. It enables individuals and computers in places with no pre-existing connectivity networks to interconnect.

The key features of MANETs are the total lack of unified authority, the absence of node association, the rapid movement of hosts, the regular dynamically changing topology of the network, the shared radio broadcast platform, the unstable operating atmosphere, the physical vulnerability and the restricted supply of resources, such as the computing capacity of the CPU, memory power, battery power and bandwidth.

Figure 1: Characteristics of MANET

Limited Battery Power
Scalability
Dynamic Topology
Low Bandwidth
Limited Battery Power
Unreliable Communications
Weak Physical Protection
Decentralized Control
Dynamic Network Topologies: The nodes inside MANETs are free to travel in either direction independently. The wireless topology of the network at irregular periods will alter constantly and arbitrarily and consists predominantly of bidirectional connections.

Low Bandwidth: These networks are smaller than fixed infrastructure networks in terms of availability and delivery range. Owing to the effects of simultaneous access, fading, noise, and intrusion situations, the throughput of wireless communication is smaller than wired communication.

Restricted Battery Power: Tiny batteries and other exhaustible sources of energy run on the nodes or hosts. Energy conservation, thus, is the most critical requirement for architecture optimization.

Decentralized control: The functionality of MANET relies on the coordination of participating nodes due to unstable connections. Thus, it becomes impossible to enforce any protocol requiring a centralized authority or administrator.

Unreliable Communications: Wireless links' shared-medium existence and unstable channel efficiency can result in a high rate of packet loss and re-routing uncertainty, which is a typical occurrence that contributes to declines in multi-hop network throughput. In wireless ad hoc networks, this means that the protection solution cannot depend on secure contact.

Poor physical protection: MANETs are more vulnerable than fixed-cable nets to physical security attacks. Mobile nodes are typically small in design, gentle and hand-held. Portable computers are becoming smaller and smaller today. They might easily get broken or misplaced or stolen and misused by an enemy. There should be awareness of the enhanced probability of multiple forms of attacks.

Scalability: When we approach a broad network scale, scalability is a crucial concern because of the restricted capacity and computing resources on mobile devices. Networks of 10,000 or even 100,000 nodes are envisaged, and one of the main architecture issues is scalability.

There are several MANET implementations.

Military Tactical Operations: In aggressive and/or unfamiliar areas, for the rapid and likely short-term establishment of military communications and troop deployments.

Search and Rescue Operations: For connectivity in regions with little to no funding for cellular networks.

Disaster Relief Operations: For connectivity in areas that are damaged or rendered inoperable with the current networks.

Law Security: During law enforcement exercises, for safe and fast contact.

Business Use: For exhibits, seminars, and broad meetings to facilitate contact. The need for collaborative computing may be more relevant outside of office settings for certain market situations than within a house. After all, it is always the situation that individuals need to hold outside meetings to work on a given initiative and share knowledge.

MANETS attacks are known as Active and Passive attacks. An intrusion in which the designated node (attacker) changes or removes data to be sent to the network is referred to as an Aggressive Attack. The assault in which the unauthorized node collects the data without interrupting the activity of the network is considered a passive attack. Security problems such as black hole intrusion, snooping attack, wormhole attack, packet duplication, routing table overload, poisoning attacks, denial of service (DoS) attacks, packet replication, and distributed Denial of Service attacks have been researched in recent years (DDoS). To address this dilemma, some of the researchers have suggested their ideas on protected routing, but the protection problem is still a big problem. Attack grouping may be achieved on a layered basis. Each layer faces attacks of various kinds. The typical attacks on different MANETS layers are shown in Table1.
Table 1 Common attack on MANETs

<table>
<thead>
<tr>
<th>S. No</th>
<th>Type of Layer</th>
<th>Different Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physical layer</td>
<td>Jamming, Eavesdropping, Interceptions</td>
</tr>
<tr>
<td>2</td>
<td>Data link layer</td>
<td>Monitoring, Study of traffic</td>
</tr>
<tr>
<td>3</td>
<td>Network layer</td>
<td>Black hole, Wormhole, Grey hole, Byzantine, message tempering, consumption of energy, floods, assaults on position transparency</td>
</tr>
<tr>
<td>4</td>
<td>Transport layer</td>
<td>SYN Flooding, hijacking Session</td>
</tr>
<tr>
<td>5</td>
<td>Multiple layer</td>
<td>Man-in-the-middle offensive, Service Denial (DoS)</td>
</tr>
</tbody>
</table>

II. LITERATURE REVIEW

V. Anjana Devi1 as well as R.S. Bhuvaneswaran [1] has proposed intrusion detection systems for cross-layer dependent Manets. To detect the event of interference, the method incorporates clustering and data mining techniques. For the clustering method, the suggested methodology implements the fixed width algorithm. The use of the fixed width algorithm allows to distinguish DoS attacks and sink hole attacks at various protocol stack layers. The proposed methods would allow use of a quick algorithm for the phase of association.

R. A new intrusion-detection device called Updated Zone Dependent Intrusion Detection System (MZBIDS) for MANETs was suggested by Santhana Krishnan, E. Golden Julie, Y. Harold Robinson, Raghvendra Kumar, Le Hoang Son Tong Anh Tuan, Hoang Viet Long[2]. Mysterious rule sharing is assured in the proposed system by bringing-in the Anonymous Location-Aided Routing in MANET in which community signatures are created by whole zone participants based on the public group key given by the leader of the intra zone. In this way, it is not necessary to show the exact location of the zone participants. The concerns with bandwidth and memory may be overcome. The method is useful for grouping the zone-based IDS in order to have a framework.

A cooperative host-based tracking method, utilising route cache data only, was suggested by Robert Basomingera, Young-June Choi [3]. It achieves an average of 95 percent detection efficiency. The suggested host-based monitoring that uses mutual data from neighbours is not just for detection but also for later protection.

Khaled Mohammed Saifuddin, Bin Ali Abu Jobayer, Ahmed Abu Shakil, Sk. Shariful Alam and Abu Saleh Ahmad[4] suggest, utilizing DSR and AODV routing protocols, an appropriate IDS for MANET based on the watchdog and path rater system. Therefore, various efficiency parameters have been evaluated to test the effects, such as packet transmission capacity, throughput, and operation delay. Several topologies available for the study have been established and they have been implemented with the proposed IDS. In addition, the MANET protection threat has been discussed and the efficiency of the IDS has been analysed using sinkhole attack routing protocols. The findings justify that malicious nodes can be marked by the suggested IDS, substituted by a false path with a valid one in the routing table, and sent to the source node.

An intruder prevention framework, Arockia Rubi.S, Dhanalakshmi.N[5], is proposed to identify malicious nodes, attackers, and fake network reports. This scheme is used for verification and to reduce the overhead incurred by pre-distribution of keys with key exchange and digital signature. A serious security vulnerability to the mobile ad hoc network is the packet falling assault. This proposed framework substantially decreases the falling of the packet and thus detects intentional fraud in instances of inaccurate reports of wrongdoing. In this method, digital signature is used to deter attackers from triggering forged acknowledgements.

Anusha K & Sathiyamoorthy E [6] provides an enhanced IDS in a MANET focused on confidence assessment and deep packet inspection (DPI). The main objective of this work is to detect network attacker nodes by finding the confidence value for each and every node. In order to initiate the route handler, the Certificate Authority creates private and public keys. Then, depending on the node's confidence score, the adjacent node authentication is done. After that, for every packet, a bogus key is computed and forwarded to the intermediate nodes. It tests whether the packet is in order after the destination receives the packet; if it is not, it is buffered, and the sequence of the incoming
packet is received. The DPI is otherwise initiated, and the packet's features are extracted. Then, it estimates the resemblance between the characteristics. The packet is compared to the intruder after calculating the similarity; if it fits, an error message is forwarded to the Certificate Authority; otherwise, the packet is forwarded to the other node.

Collaborated with Ack-based approach (ITCA), Nilesh Marathe, Subhash K. Shinde[7] suggested consolidated approach called, IDS and Trust solution Collaborated with Ack-based approach (ITCA) performs attack detection, misbehaving node isolation and network node control actions. This allows the routing mechanism more efficient by preventing malicious nodes from becoming part of a path, preventing the creation of attacks, and thereby helping to increase performance.

Ambidi Naveena & Katta Rama Linga Reddy[8] suggest a hybrid approach that uses confidentiality, one-way trapdoor protocol, hash functionality, and cryptographic elliptical curve to reduce MANET assaults. The simulation is carried out on NS-2 and the effects of the simulation on multiple measures of device execution are dissected.

Yugarshi Shashwat, Prashant Pandey, K. V. Arya & Smit Kumar [9] defines a connectivity algorithm in a MANET where, as stated in Lemma 1, there is a reasonably large possibility of packet losses for several purposes. As a consequence, it is suspected that non-malicious nodes are malicious, and their “SN Count(k)” is therefore increased. Another parameter is applied to minimize the chances of false positivity, namely “RREP Count(t)”, which increases if the node operates as usual. The node is then considered malicious and a notification is broadcast within its transmitting range by IDSs to block such a node.

J. A. Chandrasekar, Manoranjini & S. To improve the chance of discovery and avoidance of Black Hole nodes in MANETs, Jothi[10] proposes an enhanced Confidence Detection Algorithm. The proposed system uses different confidence measures to observe the actions of each node, including the interaction between sensor nodes, social and service attribute trust, and QoS metric trusts.

### III. COMPARISON OF ENERGY CONSUMPTION METHODS

<table>
<thead>
<tr>
<th>S. No</th>
<th>Authors</th>
<th>Algorithm</th>
<th>Merits</th>
<th>Demerits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>V. Anjana Devi1, R .S. Bhubaneswar[1]</td>
<td>In order to uncover malicious nodes and multiple forms of DoS, this paper suggests a successful cross-layer intrusion detection framework. This suggested solution introduces a fixed width clustering algorithm for the effective identification of MANET traffic irregularities and also produces numerous forms of network assaults.</td>
<td>Increased pace in the network for detecting the intruder can also be effectively detected compared to standard approaches and different forms of UDP flooding attack.</td>
<td>Intrusion in heavy traffic is impossible to spot.</td>
</tr>
<tr>
<td>2</td>
<td>R. Santhana Krishnan, E. Golden Julie, Y. Harold Robinson, Raghvendra Kumar, Le Hoang Son Tong Anh Tuan, Hoang Viet Long[2]</td>
<td>A new intrusion detection device, the Updated Zone Based Intrusion Detection System (MZBIDS), is suggested for MANETs. Evaluated according to contemporary methodologies, in persuaded cases, MZBIDS demonstrates superior malicious behavior-detection levels, though it does not dramatically impact the efficiency of the entire network.</td>
<td>In the case of intruders, the packet delivery ratio is improved and the false warning rate is minimised.</td>
<td>Unable to spot a larger number of assaults</td>
</tr>
<tr>
<td>Page</td>
<td>Authors</td>
<td>Title</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Robert Basomingera, Young-June Choi [3]</td>
<td>Establish a path cache sharing system for a non-clustered network where each node gathers all one-hop routing data for mutual host-based detection. A Help Vector Machine classifier is used by the cooperative host-based classification method and achieves a detection rate of about 95 percent.</td>
<td>Detecting path falsification attacks effectively</td>
<td>Restricted to just a few assaults</td>
</tr>
<tr>
<td>4</td>
<td>Khaled Mohammed Saifuddin, Abu Jobayer Bin Ali, Abu Shakil Ahmed, Sk. Shariful Alam, and Abu Saleh Ahmad [4]</td>
<td>In this article, IDS was proposed based on the watchdog and pathrater method and its efficiency assessment was provided using routing protocols for Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV) with and without taking into account the impact of the sinkhole attack.</td>
<td>Proposed routing protocols under sinkhole attack produce more throughput than DSR.</td>
<td>Restricted to just a few assaults</td>
</tr>
<tr>
<td>5</td>
<td>Arockia Rubi.S, Dhanalakshmi.N[5]</td>
<td>A new intrusion detection method utilising DSA with a key exchange algorithm is suggested in this article. This scheme is used for verification and to reduce the overhead incurred by pre-distribution of keys with key exchange and digital signature. A serious security vulnerability to the mobile ad hoc network is the packet falling assault.</td>
<td>Positive output of the proposed scheme against packet falling and disclosing fake wrongdoing.</td>
<td>In complex networks, they require precision.</td>
</tr>
<tr>
<td>6</td>
<td>Anusha K &amp; Sathiyamoorthy E[6]</td>
<td>In this article, a Trust-Based Authentication Routing with a Bio-Inspired Intrusion Detection Scheme (TRAB-IDS) is developed. The primary purpose of this article is to provide the network with protection against damaging intrusions. Here, to enhance security, the principles of confidence and deep packet inspection (DPI) are implemented.</td>
<td>In terms of protection costs, misdetection rate, latency, distribution ratio, average confidence value, and convergence review, the proposed TRAB-IDS offers better results than other strategies.</td>
<td>Need efficacy in rates of detection</td>
</tr>
<tr>
<td>7</td>
<td>Nilesh Marathe, Subhash K. Shinde [7]</td>
<td>Collaborated with Ack-based approach (ITCA), the suggested unified approach, dubbed IDS and Trust solution, performs attack detection, misbehavioral node isolation and node management behaviour in the network.</td>
<td>Providing accurate and reliable identification of malicious network nodes</td>
<td>Restricted to just a few assaults</td>
</tr>
</tbody>
</table>
3.1 Security Concerns and MANET Threats

Security has become an active research subject in the mobile ad hoc network; yet there are numerous other sharing wireless media with open network architecture, restricted capital, complex network topology and many more that impede the security of the wireless network due to self-configuring characteristics of the mobile ad hoc network. The current technologies for wired networks do not extend specifically to ad hoc cell networks.

Due to the following factors, there are numerous challenges faced to sustain protection in the mobile ad hoc network

i. Due to aggressive eavesdropping and proactive intervention, mobile ad hoc networks are more vulnerable to threats.

ii. It is incredibly challenging to incorporate the protection modules owing to the lack of Trusted Third Party adds.

iii. Mobile devices are powerless against the DoS assault because they are insufficient to operate security algorithms that need high computations such as public key algorithms due to low power consumption and computing capacity.

iv. Due to the properties of MANET, such as infrastructure-less and self-configuring, there are further chances of breaching trustworthy nodes and starting network attacks.

v. Because of the node mobility method, stale routing and bogus routing data are challenging to identify. It permits regular networking reconfiguration in the node agility mechanism, which poses further risk for assaults.

IV. PROPOSED SYSTEM

In general, MANET has two forms of protection strategies, which are intrusion prevention and protected routing techniques. An Intrusion Detection Device (IDS) is an essential part of a security infrastructure and is primarily
used to identify alleged security policy breaches by detecting and reacting to machine events that are obviously invasive. A solution is initiated to deter or reduce the harm to the device if an intrusion is observed while in the network. Several routing strategies help to protect the security of ad hoc routing. Some of them deal with thwarting ad hoc routing services and providing some solutions to help defend against these attacks, whilst other strategies seek to include some useful resources or schemes to secure ad hoc routing services against all forms of attacks. Since routing is one of the most critical network resources in ad hoc mobile networks, different forms of attacks against ad hoc routing could be evolving all the time to protect the ad hoc routing service against them. With revolutionary algorithms that cover the identification of intrusion in MANET and provide safe routing by preventing a maximum amount of security threats, the proposed scheme is focused on both intrusion and secure routing.

V. CONCLUSION

The investigator has sought to explain what MANETs are, their features and uses through this article. The different standards by which the protection of the network is measured are often understood. Crucially, the different weaknesses in MANETs are researched, and the potential attacks that can arise. The analysis of the above is well suited to consider the potential issues in MANETs. It helps to settle on an optimal way to address the issue posed. The final report on protection precautions shows the potential answers to all the issues in question. In addition, the above analysis will help researchers recognize the underlying strategies, the limitations of the current structures, and offer them a good understanding of the direction in which research could create a better framework with improved functionality.

REFERENCES