International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Trust-Based Approach to Secure Network for Malicious Nodes in Mobile Ad-Hoc Networks

[1]Deshmukh Koustubh Vivek, [2]Lokendra Singh Songare

[1]PG Scholar, CSED, Dr. APJ Abdul Kalam University Indore, M.P., India
[2]Assistant Professor, CSED, Dr. APJ Abdul Kalam University Indore, M.P., India

ABSTRACT

MANET (Mobile Ad Hoc Networking) is a rapidly developing communication framework. Because it has no foundation, MANET has the dynamic aspect of a self-enforcing network architecture. These networks need to be protected. MANET nodes can launch various attacks or become very self-centered to maintain their advantage. These nodes can be dangerous. For MANETs to function properly, malicious nodes must be found. There are many networks shown here, each with its own set of restrictions. On the other hand, this concept suggests a network of counterproductive activities based on responsive management standards. The AODV, NS-2 test network is used for performance analysis and replication. It uses a countermeasure that calculates a Trust value from the routing request, response, and data packet. After summing, assign the shares values from 0 to 1. If the trust is greater than 0.5, the node is trusted and allows access to the network. SAODV is assessed in terms of network implementation. The result is different from the standard AODV technique. SAODV outperforms AODV and existing protocols by extending the duration of throughput drops. In terms of packet delivery ratio, SAODV outperforms the earlier AODV protocol. This is a better choice than the current AODV protocol, which is vulnerable to malicious attacks.

Keyword: MANET, AODV, SAODV, CBSDV, NS2, UDP.

1. INTRODUCTION

In this section, you will offer a review of the postulation as well as its purpose. It also explains and illustrates how the problem might be described and portrayed. It is at this time when the theory's structure is revealed.

1.1 Infrastructure-less Networks

Any network, other than the simplest point-to-point connections, necessitates the use of a routing mechanism to transport packets from their source to their ultimate destinations. This involves the identification and maintenance of routes, as well as the expenditures involved with these activities. With a 'infrastructure-based' wireless network, the duty of routing is delegated to specialised nodes known as access points, which are located across the network (AP). The configurations of the APs are far less dynamic than those of their end-point nodes, which may be nomadic in nature. APs are similar to base stations in that they maintain track of nodes' affiliations and disassociations, as well as authentication and authorization, and they manage the flow of communication between their clients and between other APs. In addition, the AP may be linked to the Internet, allowing it to provide Internet connection to its customers.

In recent years, a new type of wireless networks has arisen that is built on an Ad Hoc topology. These networks are referred to as Wireless Ad Hoc Networks, and they are very appealing and promising. Wi-Fi networks are computer networks in which the communication channels are wireless, as indicated by the name wireless network. When it comes to packet forwarding and routing, the phrase "Ad Hoc" refers to the fact that there is no set infrastructure in place to do so. Figure 1.1 [2] depicts an infrastructure-based wireless network as well as an ad hoc wireless network. depicts a typical MANET (Mobile Ad Hoc Networks) configuration. The rings represent the communication ranges of the various nodes on the network. A complete circle is unlikely to exist in the actual world, and the linkages between nodes 'A' and 'B' may even be unidirectional in many circumstances — for example, although link 1 can connect node A with node B, link 1 may be unable to connect node B with node A. This might occur as a result of the signal intensities of the two transmitters being uneven, or it can occur as a result of the transmission route being different.

Because each node in an Ad Hoc network is eager to transmit data to other nodes, the decision of which nodes convey data is determined dynamically depending on the network's connection. Thisis in contrast to infrastructure-based networks, in which designated nodes, often equipped with proprietary hardware and referred to variably as routers, switches, hubs, and firewalls, are responsible for routing the data traffic between them. Ad hoc networks are ideal for use in emergency scenarios such as natural or human-induced catastrophes, military conflicts, and emergency medical emergencies, among other things, since they need little setup and can be deployed quickly. An Ad Hoc network is a temporary network that is built for a specific purpose by participating wireless nodes and subsequently dismantled.

These networks established a new art of network formation, and they are ideally suited for contexts where either the infrastructure has been lost or when building equipment is not cost-effective due to a lack of available funds

OBJECTIVE OF THE WORK

In this section, we have explained about the proposed working model and how to calculate trust value for identification malicious node.

Input: Network Scenario

Output: Find Malicious node during route discovery

Step 1: Initiate start and ending node for communication

Step 2: First start broadcast for finding the best route

Step 3: Calculate Trust value using trust calculation function

Step 4 : if (0.5<T<=1) then recheck condition

if(0.7 <= T <= 1)

Then node is most reliable

Else

otherwise, the node is only reliable

Else

Mark node is malicious

Step 5: Trust model propagate till find secure route

Step 6: Step 2 to 5 repeat until finding a secure route

Step 7: Stop

Result:-

In this part, we have shown the outcomes of our methodology, as well as the relationship between our methodology and two authoritatively existing systems, and we have determined that our process is superior to the other two systems studied. This is left to the discretion of NS-2, which will then require that the proposed framework be confirmed and confined to the degree that is reasonably possible. When it comes to both situations, the only thing that changes is the passage of time. The amount of data sent is assured in terms of bits, and this is done in a dependable manner.

Conclusion-

The major goal of this assessment will be to slow down the system's execution by maintaining a crucial separation. The evaluation will begin by alternatively maintaining the combined assault and then progress from there. The presence of the SAODV at the AODV conference is unquestionably a high point of our assessment. As this instance indicates, MANET is being attacked by more than one individual at the same time. An attack necessitates the use of NS-2 simulations in order to determine the appropriate parameters. The inclusion of both community-oriented and collaborative detrimental assaults within the criteria is required in order to fulfil the requirements. The throughput of SAODV is superior than that of AODV and the present protocol because it extends the period of time during which a decline in throughput has an impact on throughput. A much higher packet delivery ratio is achieved by SAODV compared to AODV and the present AODV protocol. SAODV's end-to-end latency is faster than both the current AODV protocol and the collaborative malicious attack AODV protocol, and it is faster than both of them.

REFERENCES

1. Umesh kumar chaurasia and Mrs.Varsha singh, “MAODV: Modified Wormhole Detection AODV Protocol”, IEEE 2013, Page No. 86-92.
2. Harleen Kaur and Neetu Gupta, "Protecting AODV from Wormhole Attack in WSN" in International Journal of Engineering and Computer Science (IJECS), vol. 3, October 2014, Page No. 8668-8672.
3. Nishant Sharma and Upinderpal Singh, “A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks" in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol.4, January 2014, Page No. 840-845.
4. S Subha and U Gowri Sankar, “Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network” in IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015, Page No. 840- 845.

5. Rakhil R and Rani Koshy, "An Efficient Algorithm for Neighbour Discovery and Wormhole Attack Detection in WANET" in International Conference on Control, Communication & Computing India (ICCC), November 2015, Page No. 1-8.

6. Amisha Parmar, V.B. Vaghelab, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network are using AOMDV protocol" in 7th International Conference on Communication, Computing and Virtualization (ICCCV) , 2016 , Page No. 40- 45.

7. Manish M Patel and Akshai Aggarwal, "Two Phase Wormhole Detection Approach for Dynamic Wireless Sensor Networks", in IEEE 2016, Page No. 1-12.

8. Manish Patel and Dr. Akshai Aggarwal, "Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information" in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 6, No.1, January 2016, Page No. 1- 9.

9. Ashish Kumar Jain, Vrinda Tokekar, "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks" , 2015 International Conference on Pervasive Computing (ICPC) , 2015 , Page No. 1-6.