International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Secure Network for Malevolent Nodes in Portable Ad-hoc Networks by Trust-based Method

Bhushan EknathMahale, Deepti Verma

PG Scholar, CSD, Dr. APJ Abdul Kalam University Indore, M.P., India

Assistant Professor, CSD, Dr. APJ Abdul Kalam University Indore, M.P., India

ABSTRACT

MANET (Mobile Ad Hoc Networking) is a rapidly expanding communication framework. Because it has no basis, the MANET has the dynamic aspect of a self-assertive network architecture. These networks need to be safeguarded. MANET nodes may launch a variety of attacks or become very self-centered in order to maintain their edge. These nodes might be hazardous. Malicious nodes must be found for MANETs to function properly. There are many networks shown, each with its own set of limitations. On the other side, this concept suggests a network of counterproductive activity based on responsive guiding standards. An AODV, NS-2 test network is employed for execution analysis and replication. It uses a countermeasure that calculates the Trust value from the route request, response, and data package. After the count, assign stock values from 0 to 1. If the trust esteem is more than 0.5, the node is trustworthy and allows network access. The SAODV is assessed in terms of network execution. The outcome differs from the standard AODV technique. SAODV outperforms AODV and existing protocols by extending the duration of a throughput decline. In terms of packet delivery ratio, SAODV outperforms the earlier AODV protocol. This is a better option than the present AODV protocol, which is vulnerable to malicious attacks.

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

INTRODUCTION

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 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

OBJECTIVE OF THEWORK

Mobile ad hoc networks (MANETs) are particularly susceptible because to their core features, which include an open medium, a dynamic topology, dispersed operation, and a limited range of capabilities. AODV is an essential on-demand routing protocol that is used often. Mobile Ad Hoc networks demand a high level of security as a fundamental necessity. The primary rationale for this thesis is that security and resilience will have an influence on the design of the standard for ad hoc networks. Investigated a malicious node detection system aiming at safeguarding the AODV protocol, which used a specification-based method to identify malicious nodes. They come to the conclusion that AODV operates well throughout a wide range of mobility rates and movement speeds. But we contend that their notion of mobility (pause duration) does not accurately reflect the dynamic topology of MANETs. The work of has been expanded upon in this thesis, and the protocol that has been developed is known as SAODV (Secure AODV).

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

CONCLUSIONS ARE CARRIED OUT:

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 kumarchaurasia and Mrs.Varshasingh, “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, VrindaTokekar, “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.