Trust Based Reliable Routing Protocol for Manets

V. Kavitha, T.Sujithra, D.Lavanya

Abstract*: *MANET contains a set of mobile nodes which communicate with each other without any underlying infrastructure and dynamic in nature. Since MANET exhibits the dynamic nature and uncentralized management, the vulnerability of security attack is more and many attacks are possible. Node misbehavior is a serious issue for routing protocols in MANET. A node may misbehave by agreeing to forward packets, and then fail to do. It leads to severe performance degradation of the network. Source and destination nodes not within the same radio range have to depend upon intermediate nodes for successful communication. Trust-based routing protocol is proposed to ensure the trustworthiness of intermediate nodes. It computes and verifies the trust for each mobile node and forwards packets on the foundation of trust. Computation of trust is based on the four different trust components such as affinity, trustworthy, energy, and bandwidth. Based on these trust values, the nodes are classified as trusted or untrusted. Untrusted nodes are isolated from the routing path and disqualified for communication. Then the key exchange mechanism is used to establish more secure communication. The data packets from the source are delivered to the destination in a secure manner that increases throughput and decreases delay since the untrusted nodes are removed from the routing path.

Index Terms*: *MANET, Multihop, Routing, Trust Computation

I. INTRODUCTION

In Mobile Ad hoc Network a set of mobile nodes communicate with each other without any central management, it provides a dynamic network configuration and does not use any underlying infrastructure. Each mobile node contains a data transceiver to send and receive the data. The transmission of the transceiver is bidirectional to enable them to send and receive data through a wireless medium. The transceiver capacity is limited to a particular distance; it can communicate with nodes that come under the wireless range of the transceiver. The advantage of the MANET is its capacity to establish communication between two or more parties without any infrastructure and allowing the parties to transfer the data while the nodes are in mobile [8]. One of the problems with the MANET is that the range of transceiver in the mobile node is limited. Hence, it can communicate with the node which is present within the range of the transceiver. To overcome the problem of the limited range of transceivers, MANET allows establishing two kinds of connection single hop and multi-hop. Direct communication is a single hop communication, when the communicating nodes are within the wireless range then direct data transfer would happen between the mobile nodes. Indirect communication can be established when the two mobile nodes are not within the communication range. In indirect communication, there are intermediate nodes which receive data and transmit the data to establish the connection between two nodes. Indirect communication is multi-hop communication.

In MANET, the communication can be established without or with minimum infrastructure, without any delay. There is no need to establish a fixed infrastructure for the communication and also, MANET supports the mobility of the communication nodes. Because of the support of mobility, dynamic nature, minimum configuration, and no delay in setting up infrastructure, it paved a way to use the MANET in emergency situations. MANET finds its application in many scenarios of disasters, including earthquakes, floods, medical emergency situations. It also used in military campaigns and in other areas where it is impossible to establish to fixed infrastructure. Since MANET exhibits easy deployment and mobility it is also used in industries.

Because of the dynamic nature and lack of central control, the MANET is vulnerable to security attacks. The characteristic of MANET is that it allows all the node to participate in the routing of data packets and all the nodes work cooperatively without a central node for the delivery of the packets. Due to these characteristics, the malicious node can be easily inserted into the MANET by the intruders. The malicious node can do both passive attacks, in which the data are monitored without any modification and the active attacks where the data is modified or the data is blocked in reaching up the destination is possible. It is necessary to concentrate on security measures for fast and secure transfer of data between the mobile nodes.

To reduce the damage to the MANET, the malicious node or the compromised node should be detected and it should be eliminated from the MANET to support secure communication. The trust-based approach to detect the malicious and compromised nodes is employed and to overcome the passive attacks in the MANET, the encryption algorithms are used. For the trust-based approach, the proposed algorithm uses the physical and logical trust metrics to calculate the trust measure for the mobile node present in the MANET. In this work, energy, and bandwidth are the physical trust parameters, affinity, and trustworthy are the logical trust parameters used to measure the trustworthiness of the node present in the network.

Revised Manuscript Received on April 18, 2019.

V.Kavitha, Department of CSE, SRM Institute of Science and Technology, Chennai, India.
T.Sujithra, Department of CSE, SRM Institute of Science and Technology, Chennai, India.
D.Lavanya, Department of CSE, Velalar College of Engineering and Technology, Erode, India.

The proposed algorithm uses the routing approach based on trustworthiness of the node to establish a secure channel between source and destination. To protect the confidentiality and integrity of data, it is encrypted using a shared secret key.

II. RELATED WORK

Liu.K et al. [9] discussed the objective of finding the misbehaving links using Two-hop acknowledgment (2ACK) scheme. In this approach, a special acknowledgment 2ACK is sent by the intermediate node in the path. If a node A sends a packet to the node B, and node B forwards the packet to the node C. Node C will send a 2ACK to node A to ensure the packet is received from node B. in 2 ACK scheme the link between the node B and node C are validated and not the node. 2ACK is sent in reverse direction only for randomly selected packets to minimize the network traffic. Node A, Node B and node C can be intermediate nodes not necessarily a destination node. This scheme can be implemented in the network layer to detect the malicious link in the MANET.

Marti.S et al. [10] described that the objective is to detect the misbehaving nodes in the MANET and reduce the usage of the node in the communication to improve the throughput of the data communication. It uses two approaches, watchdog nodes and a pathrader in each node. The watchdog is a monitoring node used to key out the misbehaving nodes and pathrater apply this information to avoid choosing a communication route through these nodes. The pathrader identifies the malicious node from the information collected and rates the node.

Patcha.A et al. [11] proposed an extended version of the watchdog to identify the malicious node in the network. The watchdog node is selected for a particular time period based on the available energy and the available storage capacity of the node. The watchdog has added the responsibility of monitoring the node for correct behavior. It uses a buffer to check whether the packet is correctly delivered by the neighbor node. It uses two thresholds suspect threshold and acceptance threshold to declare the node as malicious and good node respectively.

Roy et al. [5] proposed a distributed Intrusion Detection System (IDS) method to overcome the problems created by the selfish nodes. The selfish node uses the other node to send and receive packets but it does not participate in the routing to conserve its energy and resources. The source nodes create a mobile agent (MA) to detect the selfish nodes in the network. The MA is forwarded in the route of the packet delivery.MA calculates the Packet Delivery Ratio (PDR) of each intermediate node in the route. If a node a is node forwarding a packet and if PDR value is greater than the threshold value, MA reports the misbehavior of the node to the source node.

Anantvalee et al. [2] sorted out the IDS architecture into standalone, hierarchical, distributive and cooperative. Watchdog and path rater, CONFIDANT, CORE, OCEAN, and Cooperative IDS are some of the intrusion detection techniques discussed in this survey paper.

FenyeBao et al. [7] proposed a hierarchical trust-based system by clustering approach to detect the malicious or misbehaving nodes in the network. The network is divided into clusters, there will cluster head (CH) and sensor node (SN) in each cluster. CH will have additional resources and power. CH is elected by the nodes in the cluster. For a time interval, the CH is elected based on the election protocol. All the SN has to report the behavior of other SN in the cluster to the CH and the CH is responsible to find the trustworthy of the SN present in the cluster. CH is also responsible for identifying the trustworthy of other CH present in the network. The trustworthy of SN and CH is identified based on Quality of Service (QoS) and social trust.

Shakshuki et al. [6] proposed an Enhanced Acknowledgement scheme for IDS called EAACK. If there is no misbehaving of the node in the route then the source node will get an ACK in the given specific period, if any misbehaving is detected the source node switches to the Secure ACK (S-ACK) in which the source will get an ACK from the intermediate node. Source node to confirm the misbehavior of the intermediate node it uses the Misbehavior Report Authentication (MRA) of the source node and the destination node. Digital signatures are used to ensure the authenticity of the ACK and S-ACK sent to the source node.

III. PROPOSED METHODOLOGY

In this work, a trust-based intrusion detection mechanism is proposed to effectively detect the selfish or malicious nodes early present in the network. It uses a trust-based computation for intrusion detection and secure routing in MANETs. To evaluate the trustworthiness of the node present in the network various parameters are used in this proposed method. To evaluate the trustworthiness, the physical metric and the logical metric are considered to evaluate the overall trust of any node in the network.

A.Trust Computation

Physical trust

In the physical trust value prediction, energy and bandwidth values are taken. The present energy level of a node must be sufficient to withstand for full lengthy communication. Initially, the energy level of a node is very high. After the node starts to perform its intended work, the energy level is decreased. To evaluate the trustworthiness the energy level of the node is recorded before starting up the data communication. The energy level of the trustee node 'j' (whose trust is to be evaluated) is obtained by the trust node 'i' (which computes the trust) at the time't' as $T_{i,j}^{Power}(t)$. The energy required for successful communication is computed by multiplying the total number of packets to the ideal power consumption and receiving, processing, and transmitting power consumption [3] of the node for each packet. Energy value of a node required for successful communication, E (t) is calculated as,

$$E(t) = E_{(ideal)} + (\sum (E_{(receive)}, E_{(transmit)}, E_{(process)})) * N \quad (1)$$

where N, $E_{(receive)}$, $E_{(transmit)}$, $E_{(process)}$ are the number of packets in a communication, receiving, transmitting, and processing power consumption by a node for each packet respectively.

It is necessary to ensure that

$T_{i,j}^{Power}(t)$ is greater than E(t) for successful communication.
Bandwidth measure gives the number of packets transmitted in a given time higher the bandwidth, more number of packets is transmitted. Hence, bandwidth is regarded as an important thing in measuring the QoS of any route in the network..The data transmission rate between any two nodes should ensure before evaluating the physical trust of the network. Available bandwidth on the link (i, j) [4] is estimated at time‘t’ as $T_{i,j}^{Bandwidth}(t)$.

Logical trust

In the logical trust value prediction, affinity and trustworthy values are taken. The affinity value is related to the number of past interactions that a trustor node ‘i’ made with the trustee node ‘j’. Initially, the affinity value is set to 0. If a node ‘i’ transfer a packet to the neighbor node ‘j’ in the network. If the packet traveling through node ‘i’ and node ‘j’ reaches the destination node successfully the node ‘i’ increases the affinity of node ‘j’ by +1. Successful communication is confirmed by ACK sent by destination. Otherwise, the value is decreased by -1. It is calculated at time ‘t’ as $T_{i,j}^{Affinity}(t)$ after a certain number of interactions.

If the node enters and leaves the network on proper request, it increases the trustworthy value of a node by +1. Otherwise, if node suddenly leaves the network without any proper intimation, the trustworthy value of a node is decreased by -1. It is calculated at time‘t’ as $T_{i,j}^{Trustworthy}(t)$.

The node ‘i’ computes the trust value of the node’j’ at a given time t is based on the parameters of power, bandwidth, affinity and trustworthy of the node ‘j’ and is defined by Equation (2).

$$T_{i,j}(t) = \sum (T_{i,j}Power(t), T_{i,j}Bandwidth(t), T_{i,j}Affinity(t), T_{i,j}Trustworthy(t)) \quad (2)$$

If the overall trust value $T_{i,j}(t)$ is less than the predefined threshold, then it is marked as an untrusted node. Otherwise, it is declared as the trusted node for communication.

B. Trust based routing

Each node computes the trust value for its 1-Hop neighbors. After the computation of trust, nodes are classified as trusted or untrusted. To establish secure communication, a route is established from source to destination through only trusted nodes and untrusted nodes are isolated from the communication path. The source node initiates a route discovery process by using DSR routing. DSR routing protocol may find multiple routes to the destination in the MANET. From the received multiple routes to the destination the source node selects the route which has the maximum value of trustworthiness. Similarly, intermediate nodes select the next hop with the highest overall trust value and transfer data through the route. The node’s trust value is updated on demand when the data transfer has to take place.

C. Key Generation

The secret key is exchanged between the source and destination which makes data transmission more secure. It uses Diffie - Hellman algorithm for key exchange. It is a specific method of exchanging cryptographic keys. This enables a pair of nodes to share a secret key between them to make secure communication. In Diffie - Hellman the source node and the destination calculates the shared key at their ends. The data communication is done by sending the encrypted data using the shared keys. The sender encrypts the data using a secret key and transfers it to the next hop. This transfer process takes place repeatedly and data reaches the destination. It decrypts the received data with shared secret key.

IV. PERFORMANCE EVALUATION

A. Performance Metrics – PDR, RO

The proposed protocol is measured based on the parameters listed below:

Control overhead: The control overhead is the overhead occurred due to the transfer of control packets in the network and it is calculated as the number of control packet transferred to the total number of packets received.

Average end-to-end delay: The end-to-end-delay is calculated by averaging all the end-to-end delay of the successfully delivered packets in the destination.

Average Packet Delivery Ratio: The ratio of the number of packets received at the destination to the total number of packets sent from the source.

B. Analysis

The use of Diffie-Hellman exchange allows to share the secret key through the unsecured channel and the cryptographic function are done only at the source and the destination nodes and it does not add any overhead at the intermediate nodes present in the routing path. The control overhead is kept to minimal by using the monitoring of only the neighboring nodes and reporting to the source node at a given time interval. For sensitive networks, the time interval can be decreased to ascertain early detection of malicious nodes. The average end-to-end delay is kept minimal by selecting the path which is most trustworthy considering the bandwidth for good QoS. The average packet delivery ration is maximum since for every route selection the trustworthiness and the bandwidth are considered.

V. CONCLUSION

Due to the wireless connections and decentralized administration, MANETs need more security than wired networks. The packet dropping attack a kind of active attack is the major security issue faced by the MANET. The design of the proposed system, a Trust based routing protocol is specially designed for MANETs. It takes energy, bandwidth, affinity, and trustworthy values as trust parameters and computes the overall trust of a node. Data transfer takes place through trusted nodes, which ultimately improves PDR, reduce routing overhead and preserve battery power of nodes.

REFERENCES

1. Abdalrazak T. Rahem, H. K. Sawant , "Collaborative trust based secure routing based Ad-hoc Routing protocol," International journal of modern Engineering research, vol. 2, Issue. 2, pp. 95-101, April 2012.
2. T. Anantvalee, and J. Wu, "A Survey on Intrusion Detection in MobileAd Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
3. S. Aravindh, R. S. Vinoth, and R. Vijayan, "A Trust based approach for detection and isolation of malicious nodes in MANET," International journal of Engineering and Technology, vol. 5, no. 1, pp. 193-199, March 2013.
4. Cheikh Sarr, Claude Chaudet, Guillaume Chelius, and Isabelle Guerin Lassous, "A node-based available bandwidth evaluation in IEEE 802.11 ad hoc networks," International Journal of Parallel, Emergent, and Distributed Systems, pp. 1-21, July 2005.
5. Debdutta Barman Roy, and Rituparna Chaki, "MADSN: Mobile Agent Based Detection of Selfish Node in MANET," International Journal of Wireless & Mobile Networks, vol. 3, No. 4, pp. 225-235, August 2011.
6. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK - A secure Intrusion Detection System for MANETs," IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089-1098, March 2013.
7. FenyeBao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.
8. Imrich Chlamtac, Jennifer J. N. Liu, and Marco Conti, "Mobile ad hoc networking: imperatives and challenges," Elsevier, pp. 13-64, 2003.
9. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.
10. 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. 255-26, 2000.
11. A. Patcha, and A. Mishra, "Collaborative security architecture for blackhole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., pp. 75-78, 2003.

AUTHORS PROFILE

V. Kavitha is currently working as Associate Professor in Department of CSE, School of computing, SRM Institute of Science and Technology, Kattankulathur, Chennai, India. She has completed her Doctrol degree in 2018 from Anna University,Chennai. She has done her Master Degree in CSE in Anna University Coimbatore in 2009 and BE in CSE under Madras University in 2001. She has 12 years of teaching experience. She has presented papers in many international and national conferences. She has published her research articles in more than 10 journals.

T.Sujithra, received her DECE degree in electronics and communication engineering from DOTE in 2005. She received her BE degree in Computer Science and Engineering from Anna University,Chennai in 2008. She completed her Masters degree in Computer Science and Engineering from Anna University, Chennai in 2012. She was awarded with PhD from Anna University, Chennai in 2017. She is presently working in Wireless Sensor Networks, IOT and Data Mining. She is currently Assistant Professor in the Department of Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India.

.

D.Lavanya has completed her Bachelor's degree in Information Technology from Anna University in the year 2009 and Master degree in computer science and engineering from Anna University, Chennai in the year 2014. She is currently working as Assistant professor in the department of Computer Science and Engineering at Velalar College of Engineering and Technology.