Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Enhanced Approach for Trust Based Routing in MANET

P. L. N. Murty, Gagandeep Singh
Lovely Professional University,
Jalandhar, Punjab, India

Abstract: ***MANETS does not have any fixed topology and the nodes move from one location to another. To transfer a packet from sender to receiver it should follow a routing mechanism and data can be transferred securely such that the route should be trusted and nodes could not be compromised. In this paper we discuss about an enhanced approach for security in trust based routing algorithm by considering AOMDV as ET-AOMDV which is a multipath routing. We implement rail fence technique on the message and further encryption technique is performed and passed over the network to reach to its destination***

Key terms- MANET, trust model, encryption, DSR routing, disjoint AOMDV, performance, simulation

I. INTRODUCTION

Mobile adhoc networks are increasing now a days as there were many technologies like zigbee, wimax and many network oriented technologies. Mobile adhoc networks does not have fixed infrastructure and there is random change of topology due to mobility. As there is no fixed topology the nodes can be trusted or not secure. To transfer the message from source to destination some routing techniques are followed. The message is made into different packets and sent over an independent path in the network.

Here we discuss about an enhanced trust based routing algorithm, which is processed by using AOMDV or DSR as it is defined as ET-AOMDV or ET-DSR. Here the process is done by a enhanced trust based routing with some encryption techniques at the sender end and decryption at the receiver end . Mainly this algorithms contains three phases namely (1) encryption- where the message is divided into some fixed number of parts which is defined to be shares and it will be calculated .(2) message routing – the data is sent over the network by using an routing algorithm by using the data packets independently into the network such that no node will be get effected or compromised by using an AOMDV or DSR routing algorithms.(3).Decryption – as the message parts are received to the destination then the receiver keeps in order according to the packet serial number and he converts the cipher text into plaintext and finally message will be obtained .We consider a trust management model of the node such that we can find the affected paths and nodes in the network.

The remaining paper contains as Section II as literature survey, section III as related work, section IV as proposed scheme, section V – we finally conclude our work.

II. RELATED WORK

Many routing schemes have been implemented such that the data can be passed to destination very easily or without any problems. The routing protocols are broadly classified into three categories they are proactive, reactive and hybrid routing techniques. Some of the attacks that can occur while possessing the routing or information transfer. The attacks are broadly classified into active and passive attacks. In passive attacks the data cannot be altered and in active attacks it is difficult to find that which data has been altered in the message. Some of the methods are present to detect the malicious nodes or nodes with low behavior. The node can be trusted by some of the following mechanisms are credit based, trust based, friend based and reputation based and secure based AODV protocol. To deliver a packet to the destination we follow several methods. As there is no fixed topology in the Manets the nodes may move from one location to another location due to this the topology changes – frequently topology changes. By using the cryptographic algorithms and multipath routing techniques the packet will be delivered securely and in efficient way.

Isaac Woungang, 2011 – This paper mainly deals with multipath routing with software encryption to transfer the messages very securely over the network. This approach mainly contains three phases. They are

i. Encryption: The message is divided into some segments and those segments are done by XOR operation to get the cipher text which is encrypted text.

X = a XOR c Y = b XOR c

Z = a XOR b XOR c

ii. Decryption: After the packet is received with the cipher text to the destination, we decrypt the cipher text to get the original text and can be calculated as

a= Y XOR Z

b= X XOR Z

c = X XOR Y XOR Z

iii. Message Routing: Where the message can be passed through various independent nodes and delivered to the destination by using various trust models. Trust mechanism and secure routing are used to get the trust values of the nodes and maintained in the trust table. The trust value of the node is calculated as delivery of packet is success or failure. A secure routing is performed by using the multipath algorithm AOMDV in the routing process.

Isaac Woungang, 2012 – This paper mainly explains how to implement an enhanced trust based multipath dynamic source routing [ETB – MDSR]. This model mainly consists of soft encryption, novel trust management strategy and multipath DSR routing. Manet have information exchange and delivery of packets can be performed without any pre existing infrastructure of the fixed network. Manets gives a certain level of cooperation which occurs among the nodes before the routing occurs. Some of the solutions had been done for the secure transmission of packet are Credit based systems will be performed by giving the credits values to the nodes in the process of forwarding the data. Reputation based systems, where we use the node reputation as parameters to find the well behave nodes and to drop or remove bad nodes. The well behave nodes participate in data forwarding of packets..Cryptographic based system is used some encryption techniques to secure the data. Multi path secured routing is defined as where the data will be splits into some parts before transferring and encryption is performed further routed in the available paths.

In TB- MDSR, it took more time to find multiple trust paths based on secure data transfer. The trust value can be computed by using the direct computation. If the data is not suitable for direct computation then indirect computation is performed. The trust value of a node can be calculated as the interactions with the neighbours and recommendations. These mainly show a wish to the other nodes which may be treated as malevolent nodes in credit based systems , where as in reputation based mainly keep the track of all neighbours to punish the bad nodes and remove it and its value . In TFT a bad node decreases it service and lower the performance, that in which it did not involve in transferring the packet, main disadvantage in this is boot strapping. In cryptography these implement security in Manets but the key mechanism which used was different. Process of passing the data is explained as following

Step 1: Message is split into some parts and transfer from source to destination. The shares are routed among trust paths.

Step 2: A route will be selected by using the trust management model. The trust model describes the trust values in the form of levels as from -1 to 4 where 4 describes as complete trust with high recommendation and -1 describes it as completely distrust where the packet to be dropped.

The more encrypted parts cannot be transfer through that node depend upon the assigned trust value. Non trusted routes can be avoided which can be done by the brute force attacks.

In ETB-MDSR, the routing will be performed based upon the management model where the remaining process is continued as the TB-MDSR. History of interactions stores the data of process between the nodes. The HI value can be updated by using the HI module. TC (trust computation) selects the data value and checks to perform which type of computation. This can be mainly decided by the level of confidence, where the satisfying and unsatisfying interactions are calculated. If the confidence value is greater than the threshold value then direct computation is performed. If the confidence is less than the threshold value indirect computation is performed. TC module uses the filtering method to get the honest recommendations and weighting method. TC can be calculated as the sum of violation for the path selecting routing. Trust values can be converted in the range of (x,y). The trust compromise of TBMDSR is always zero. If the malicious node increases then this protocol take less time to find the path. When the velocity increases then route selection time decreases. This protocol takes less time for finding the route than TB-MDSR.

III. PROPOSED SCHEME

Enhanced approach for trust based scheme:

As a enhanced approach to the trust based multipath routing we discuss the proposed scheme as follows

A. Path trust by path computation

To deliver a message from source to destination or a from node to node we should follow a path by implementing a routing scheme. The path can be defined by giving its trusted value by getting up the path cost such that the nodes that are involved in that path. Path cost can be calculated and it can be define to be path trust. The trust value can be various levels and values are assigned to it as 4 to -1 where it can be defined to be that the trust with value 4 has complete trust with high recommendation and the value with -1 is that

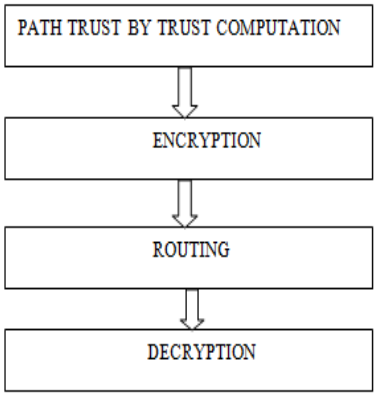

Figure: Proposed scheme

distrust value such that it drops the packet .The path with low trust can be defined to be it have a no trust means that the packet which are transferred through this path can be affected and gets compromised. We can define the range of trust values into group of classes such that the nodes with this trust belongs to this class range and level where each and every path must have some minimum trust value to select the path.

B. Encryption

Initially the message which we want to transfer over the network is taken and a cryptographic technique rail fence technique is used and after applying the rail fence the encrypted content is embedded into single content and further the content is divided into some parts known as shadows or shares as we propose them to define into three equal shares if any extra character beyond the length then we consider the null character to be placed in the text and we perform a encryption process as follows

$$a^1 = a \Theta c$$
$$b^1 = b \Theta c$$
$$c^1 = a \Theta b \Theta c$$

C. Decryption

When the message is received at the receiver end then the receiver must perform a decryption process by decrypting them. After the message is decrypted we perform a derail fence technique which is quite vice versa to the rail fence technique and then the message is amended according to the sequence number of the shares and the decryption can be done as follows

$$a = b^l \Theta c^l$$
$$b = a^l \Theta c^l$$
$$c = a^l \Theta b^l \Theta c^l$$

D. Message routing or secure routing

Here we perform the routing by considering the two aspects such as the trust mechanism and secure routing as follows.

Trust Mechanism: The trust value of a node can be depended upon the delivering of packets. The node which delivers more packets then its trust value will increase, if a node has more chances of failure of packets then trust value will decrease. If trust value is less than the threshold trust value then malicious nodes can be easily detected and message can be compromised .The trust value of a node can be calculated as T = W1 * DT + W2 * TR. Where W1, W2 are weights assigned to the nodes and DT is the direct trust value, TR is the trust recommendation value. Success value is calculated as S and failure value is calculated as F, C is constant.

DT = DT + (C* S) (for success nodes)

DT = DT – (C*F) (for failure nodes)

When the node is transferred successfully then S is incremented by 1 or reset to zero. When the transfer fails then F will be incremented by 1. The values can be computed by monitoring of AOMDV packet forward process. HELLO packets are used to determine trust value such that when a message is received then it checks in table and find the nodes. If any node exists then it will receive a message. The trust of the path is calculated as the

$$T_{AC} = 0.1 * T_{A \rightarrow X} * T_{X \rightarrow C}$$

If node A wants to transfer the packet to the destination node C then it should follow the route through node X which is an intermediate node for node A and C. Path trust is calculated as, if the trust value for the path A to X is 9 and trust value for the path from the path X to C is 6 then the trust recommendation value for the path A -> C is 0.1 * 9 * 6 =5.4 .The trust values of the routes are calculated based upon the trust table.

Secure routing: When a source sends a request packet to the following node to deliver at the destination, it checks the hop count from the source node and sends a reverse path where the hop count will be recorded. After the packet is received to the destination then it sends reply packet through the nodes, if it sends a route error message then the path will be discarded. When the node will send the data RREQ packet to find destination it again sends reply packet and it compares the trust value of the node and reserved trust value. If the node trust is less than the reserved trust then it will be replaced by neighbor trust and further packet if forwarded.

After the source receives all the trust values and reply packets then routing will be performed. If a path is selected but it was not suitable to transfer data then the process will start again by considering other path.

IV. CONCLUSION

In this paper we are proposing a new technique on a T-AOMDV to increase the security in the packet and node such that it cannot be compromised by having some cryptographic schemes and trust based activities where we used a various cryptographic algorithms.

REFERENCES

[1] Multi Path Trust Based Secure AOMDV Routing in Adhoc Networks – Jing Wei Huang,Isaac Woungang,Han – Cheih Chao ,Mohammed S.Obaidat (IEEE Globe com 2011)

[2] Trust Based Adhoc On Demand Routing Protocol for MANET - Naveen Kumar Gupta , Kavita Pandey (IEEE 2013)

[3] Trust Enhanced Message Security Protocol for Mobile Adhoc Networks – Jing Wei Huang,Isaac Woungang,Han – Cheih Chao ,Mohammed S.Obaidat (IEEE ICC 2012)

[4] Light Weight Trust Based on Demand Multipath Routing Protocol for Mobile ADHOC Networks – Chuanhao Qu, Lei Ju, Zhiping Jia, Huaqiang Xu, Longpeng Zheng (IEEE 2013)

[5] SPREAD : Enhancing data confidentiality in mobile adhoc networks – W.Lou , W.Liu ,Y.Fang (INFOCOM 2004) .

[6] Split multi path routing with maximally disjoint paths in adhoc networks – S.J.Lee , M.Gerla (ICC 2001) .

[7] On the impact of alternate path routing for load balancing in mobile adhoc networks – M.R.Peralman , Z.J.Haas, P.Sholander , S.S.Tabrizi (MobiHoc 2000) .

[8] Multipath routing in the presence of frequent topological changes – A.Tsirigos, Z.J.Haas (IEEE 2001).

[9] Predictive caching Strategy for on Demand Routing Protocols in Wireless Adhoc Networks – WENJING LOU and YUGUANG FANG (2002)

[10] K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, E. M.Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proc. of 10th IEEE Intl. Conf. on Network Protocols, Paris, France, pp. 78-89, Nov. 12-15, 2002

[11] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing", Computer Communications, Vol. 31, pp.760-769, 2008s

