International Journal on Applicationsin Information and Communication Engineering
Volume 2:Issue 5: May 2016, pp 65-69. www.aetsjournal.com ISSN (Online) : 2394 - 6237

Trust Based Co-Operative DSR Routing Protocol for MANET

K.Nishanthi, R.Vijayakumar

***Abstract*——**Mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. The networks work well only if the mobile nodes are trust worthy and behave cooperatively. Due to the openness in network topology and absence of a centralized administration in management, MANETs are very vulnerable to various attacks from malicious nodes. In order to reduce the hazards from such nodes and enhance the security of network, The proposed work presents a dynamic trust model to evaluate the trustworthiness of nodes, which is based on the nodes historical behaviours and future behaviour and the proposed trust predication model have been integrated into the Source Routing mechanism termed as Trust based co-operative Dynamic Source Routing protocol which provides a flexible and feasible approach to choose the shortest trust worthy route that meets the security requirement of data packets transmission by isolating the malicious nodes. Experiments have proved the efficiency and effectiveness of the proposed mechanism in malicious node identification. The results show that the proposed system improves packet delivery ratio and reduces average end-to-end latency. The proposed model is simulated using Network Simulator (NS2).

***Keywords*—** MANET,trustvalue,trustworthiness,malicious node

I. INTRODUCTION

A Mobile Ad hoc Network is a collection of wireless mobile nodes forming a temporary network without any infrastructure or centralized administration (Chansu Yu et al 2003). Ad hoc wireless network is comparatively a new paradigm of multi-hop wireless networking and has become popular. It is an essential part of the computing environment, consisting of infrastructure-less mobile networks. In MANET, each node communicates with other nodes directly or indirectly through intermediate nodes. The credit for the growth of ad-hoc network goes for its self organizing and self configuring properties.This kind of network is well suited for mission critical applications such as emergencyoperations,military applications. All nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. Because of no centralized management securing a mobile ad -hoc network is very challenging, there exist some potential loopholes and vulnerabilities in MANETs that can be attacked and exploited by the malicious and undesirable nodes to disrupt the smooth functioning in the network

K.Nishanthi, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India . (Email :nishanthi.nishavishnu@gmail.com)

R.Vijayakumar, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India. (Email : vijayakumar.r@gmail.com)

A. Trust management mechanism

Trust describes a subjective relation between an entity and another entity (or group of entities) while reputation is what is generally said about an entity.Trust may be used to determine the reputation of an entity. Trust management mechanisms have grown as an effective tool for evaluating the trustworthiness of the entity in several distributed systems like e-commerce, social networks and mobile ad hoc network environments. The main aim of using the trust mechanisms in a network is to assess the trustworthiness of the nodes participating to form a active path for communication and to detect and isolate the malicious nodes to discourage the bad behaviour of the participating nodes which degrades the network performance.

B. Ad-hoc on Demand Routing Protocol

In ad-hoc on-demand routing protocol routes are created only as and when needed. The source node invokes the route discovery process only when the data packet has to be transmitted hence the message overhead is reduced.The source node stores the next-hop information of the intermediate nodes till it reaches the destination for data packet transmission.

If a possible route is not found to the destination then the route-request is flooded over the network.

C. Dynamic Source Routing

Dynamic source routing protocol (DSR) is an on-demand routing protocol. It is a source routed protocol.Under DSR protocol, as mentioned in [2] [6] all control packets contain transmitted for pathdiscovery for the complete list of nodes that form a route to destination node D. Source node S broadcasts a route REQUEST (RREQ)packet containing a unique identification number and the IP address of D. When it receives first copy of the RREQ packet, a node that has no route to D appends its IP address to the RREQ packet and rebroadcasts it. When a RREQ reaches to the D, a node which has a route to D, a route Reply (RREP) packet that contain the IP address of every node forming the route is returned to S. Several RREP packets can be issued by D. Nevertheless, a node forwards only the first RREP packet it receives and consequently multiple node disjoint paths can be established between S and D. If a link brakeage occurs and results in the

incapacity of forwarding, node to reach the destination, a route ERROR (RERR) packet is sent to the source. All nodes that have no alternate path to D update their routing table according to the RERR packet information and forwarded the RERR packet to S

II. Related Work

In [7]Michiardi,&Molva introduces collabrative reputation mechanism to enforce node cooperation in mobile adhoc-networks is based on collabrative monitoring technique. CORE divides the reputation of node into three distinct components.Subjective reputation based own observations,Indirect reputation based positive report produced by another node Functional reputation based on behaviour monitored during a particular task. CORE scheme can be used to monitor the Packet Forwarding (PF) function. Once a node has obtained a valid route to the destination through the DSR Route Discovery function, it can start sending data packet to its target. Each network entity belonging to the path from the source to the destination has to perform the PF function in order transfer the data packets. This mechanism can be used to detect any misbehaving nodes that refuse to cooperate to the PF and the evaluation of the reputation value reflects any node misbehavior. The execution of the PF function is granted for any node classified as a cooperating entity while it is denied for misbehaving nodes.

Li, X., Jia, Z., Zhang,Zhang, R, & Wang [8] propose a trustbasedondemand multipath routing protocol in whicha source can establish multiple loop-free paths to a destination in one route discovery process. Each path has an evaluation vector composed of a hop count and a trust value. A node is considered as malicious based on its forwarding behaviour. This protocol is able to discover multiple loop-free paths as candidates in one route discovery. The paths are evaluated by two aspects known as hop counts and trust values. This two-dimensional evaluation provides a flexible and feasible approach to choose the shortest path from the candidates that meet the requirements of data packets for dependability or trust. It enhances the dependability of forwarding packets and alleviates the threats from malicious nodes.

Farruh Ishmanov [4] proposes aaSecure Trust Establishment Scheme for Wireless Sensor Networks.Anovel trust estimation method is proposed that is robust against on-off attacks and persistent malicious behaviour. The proposed scheme combines past misbehaviour with current status in a comprehensive way. Trust is calculated based on either past interactions or past recommendations. A past interaction–based trust estimation method considers three factors to estimate the current trust value such as current measured misbehaviour, aggregated misbehaviour, and previous trust value. Current measured misbehaviour shows a node's behaviour during the current time, whereas aggregated misbehaviour and previous trust value demonstrate how much a node has misbehaved in the past. Aggregated misbehaviour which aggregates measured misbehaviour over time using proposed method. It shows the persistency of the misbehaviour. So, according to our proposed method if measured misbehaviour is persistent, that is, it is always greater than predefined threshold, then each time aggregated misbehavior will be increased until it reaches to maximum value(that is one).

MuneerBani Yassein,2012)[14] proposes a new mechanism to improve the performance of routing protocol against the malicious attacks. The proposed protocol, named trust Schemeaims to detect malicious nodes in MANETs and then avoids transmitting messages through them. Therefore, nodes transmit data via trusted paths to enhance network performance. The Trust Scheme evaluates the behavior of all nodes by establishing a trust value for each node in the network that represents the trustworthiness of each one. It calculates the trust value of a node by directly observing the behavior of the node and then passing this value with other observations from other nodes in the network. The behavior of the neighboring nodes is used as an indication to distinguish between normal nodes (nodes that act as expected) and malicious nodes. If an estimated trust value is under the trust threshold in persistent misbehaviour or an on-off attack, we consider that misbehaviour or attack have been detected.

Pirzada,,MCdonald [10] proposes a Dependable dynamic source vector routing without a trusted third party for discovering discovering and maintaining dependable routes in MANET and also integrates the trust prediction model into the source routing mechanism. Number of attacks may be launched against the DSR protocol, which leads to the malfunction of the network usually at a critical point in time. A novel technique of discovering and maintaining dependable routes in an ad-hoc network even in the presence of malicious nodes. Each node in the network monitors its surrounding neighbours and maintains a direct trust value for them. The trust values are associated with the nodes present in the DSR link cache. To compute the direct trust in a node an effort-return based trust model is used. The accuracy and sincerity of the immediate neighbouring nodes is measured byobserving their contribution to the packet forwarding mechanism. Every time a node transmits a *data* or control packet it immediately brings its receiver into the promiscuous mode, so as to overhear its immediate neighbour forwarding the packet to compute the trust in a node. This filtering process ensures that all packets destined towards a malicious destination or traversing a malicious node are not permitted to propagate in the network.

III. Proposed System

The proposed protocol, named Trust Scheme, aims to detect malicious nodes in MANETs and then avoids transmitting messages through them. Therefore, nodes transmit data via trusted paths to enhance network performance.The Trust Scheme evaluates the behavior of all nodes by establishing a trust value for each node in the network that represents the trustworthiness of each one. It calculates the trust value of a node by directly observing the behavior of the node and then passing this value with other observations from other nodes in

the network. The Each node in the network observes the behavior of its neighbors. It observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboring nodes, and the past activity of the node. Those parameters are then used to determine which nodes are misbehaving in the network. The behavior of the neighboring nodes is used as an indication to distinguish between normal nodes (nodes that act as expected) and malicious nodes. Then, the observer node builds a table that records a local trust value for each neighboring node estimated from these observations. We note that only using the trust value in may not be an accurate measure to decide that a node is a malicious one. Therefore, each node constructs a closeness Trust Table that stores the trust value for all nodes not only the neighbors but also the far ones. If any node having the trust value less than 1,the node is detected as malicious and is isolated from the active path of the network. The energy value is calculated after calculating the trust values for each node. Every node has some initial energy before transmission. When the mobility and processing takes place energy value decreases accordingly. Every mobile node consumes energy to transmit a packet, receive a packet and to overhear the neighbor nodes. The remaining energy value for each node is calculated by reducing the energy consumed by the node from the initial energy. The source node checks for availability of any existing path for destination, then the average trust value for the path is calculated. The source node sends request for destination along with the trust value. The shortest path with high trust value and remaining energy is selected as route for transmission.

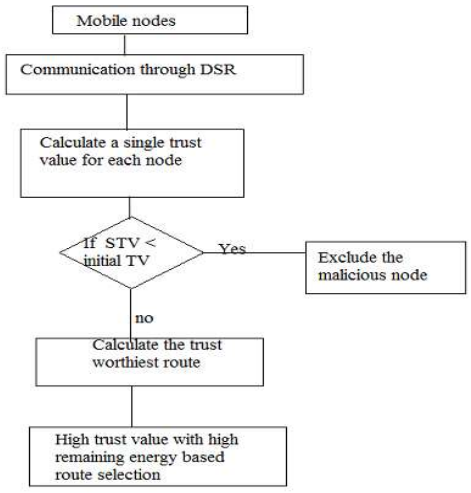

Fig.1 The architecture of the trust based mechanism

1) System Assumptions

There are certain assumptions defined are as: a) Every participating node in the network must install its Multi Agent System (MAS) which consists of monitoring agent (MOA) and routingagent (ROA). b) All the trust computations‘ are maintained locally the nodes MOA. c) The agents are re4bound to unauthorized analysis and changes of their computation and messages.

A. Node Trust Value Calculation

Initially all nodes in the network is assigned with an initial trust value one. Every node maintains trust value of its neighbour node. For fixed time intervals the single trust value is calculated for neighbour nodes. A node calculates the trust value of its neighbour node by listening promiscuously. For calculating the trust value of the neighbour node the packet forwarding behaviour of the neighbour node is considered. The trust value of a particular node is based on subjective assessment by the agent node about the packets received and transmitted by the node at a given situation and given time. The ATDSR guarantees that there is always a single trust value for each node in the network. It gives quite an accurate estimation about the trustworthiness of a node. In addition to that, the nodes themselves are able to provide their own trust information whenever requested; therefore, trust computation is done without network wide flooding and with no acquisition-latency. To reflect this kind of node’s ‘‘selective forwarding’’ behavior compute Trust_Value (M) as:

$$\textbf{Trust value}(M) = \frac{SF(M)}{RF(M)} \quad (1)$$

where, RF(M): The total number of packets that all nodes have transmitted to node M for forwarding;

SF(M): The total number of packets that have been forwarded by node M;

The value of RF(M) is incremented by one everytime a node have transmitted to node M for Forwarding and the value of SF(M) is incremented by one everytime when a node successfully forwards the packet of node M.

B. Calculation of trust evaluation table for each node

For each arbitrary node Ni, its MOA, locally maintains a trust evaluation table Teval (N). The trust evaluation table Teval (N) contains the trust value of other nodes in the network. ATDSR depends on transferring the trust values of nodes through the Route Request packets in addition to the routing information, each Route Request (RREQ) packet contains a trust record in which is accumulated a record of the sequence of hops taken by the RREQ packet as it is propagated through MANETs during this Route Discovery process. For each node acting as a forwarder during the Route Discovery process, its routing agent ROA is responsible for appending the computed trust value of that node to the RREQ packet that was sent by the preceding node. In this manner, when a RREQ packet is sent, it carries the trust information about each forwarding node which is shown in fig

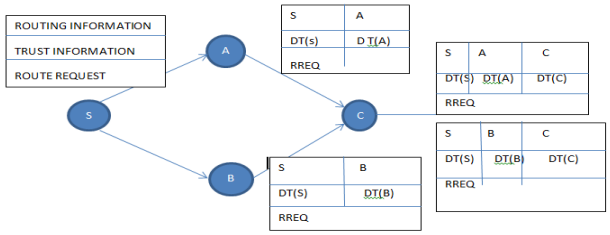

Fig 2Trust value propogation

If the calculated trustvalue is less than the initial trustvalue then the node is detected as malicious and it is isolated from the active path of the network.

C. Trust worthy route calculation

Using the trust information, the sending node routing agent ROA(S) is responsible for computing the most trustworthy route to a particular destination. If the most trustworthy route trusts value is found lower than a threshold value (denoted by Rthreshold). The route is rejected and a new Route Discovery process is initiated. The trust value in route R by source node S is represented as Ts(R) and given by the following equation:

$Ts(R)=\min(Trust\_value(N_i))$ N_i belongs to R

D. Trust and energy based route selection

The source node checks for availability of existing path for destination,and if there is average trust value for path is calculated. Then the shortest path with the high trust value is selected as a trustworthiest active path for communication.Inorder to exclude malicious node single trust value of each node is calculated based on the forwarding behaviour of the nodes. The trust value computed is compared with the initial trust value assumed if it is less then the malicious node is excluded if it is equal are higher then that node is selected for transmission based on trust and available energy to transmit the packets.

IV. Experimental Setup And Results

The overall aim of the experimental simulation is done using network simulator is to measure the accuracy of the proposed trust based routing protocol

Parameter	Value
Packet size	2000 bytes
No. of Nodes	40
Protocolused	DSR
Dimension	1000*1000
ChannelType	Wirelesschannel
	IEEE802.11
Queue Type	Drop
	Tail/PriQueue
Antenna	Omni Antenna
Protocol	TCP
Mobility	10 m/s

Fig 3 Simulation scenario

To validate the efficiency of the proposed method against attacks due to malicious nodes and to analyse the network performance using NETWORK SIMULATOR (NS2)

A. End-To-End Delay

The average time taken by a datapacket to arrive in the destination. It also includes the delay caused by route discovery process and the queue in the packet transmission.Only the data packets successfully delivered to destinations ar counted.

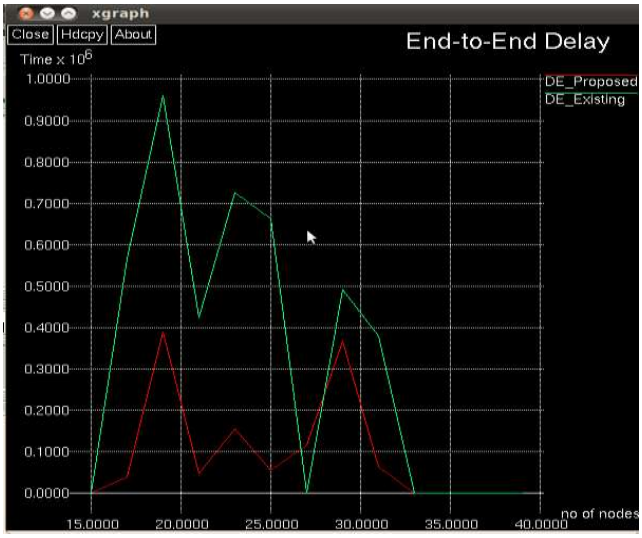

Fig 4 End to End delay

Fig 4 shows the average end to end delay of the proposed architecture.

B. Average Energy Consumption

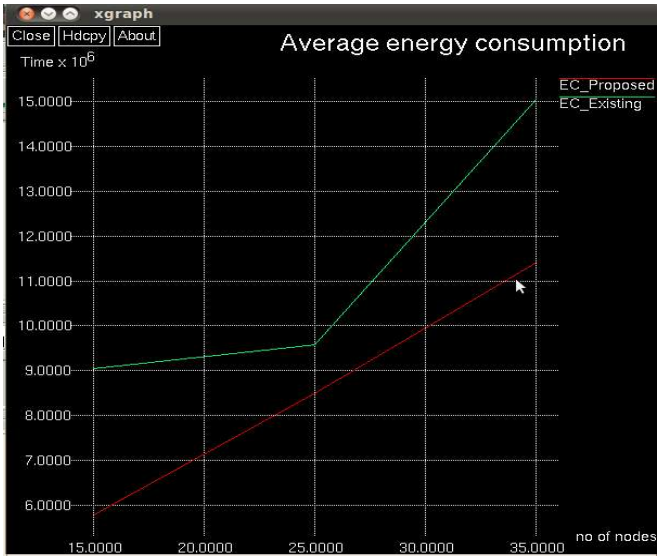

Fig 5 Average energy consumption

Fig 5.shows the average energy consumed during the route selection process by the proposed system

V. Conclusions And Future Work

From the above comparisons it is concluded that the proposed system performs better in detecting and isolating the malicious nodes and the packets are correctly forwarded to the destination by decreasing the end to end delay and energy consumption has been reduced. In future,security mechanisms can be implemented for transmission. Various encryption methods can be used to attain security mechanisms.The proposed trust based mechanisms can be incorporated in different on-demand routing protocols and also other proactive routing protocols.

REFERENCES

[1] Alireza, A., et al. (2012) A survey of security challenges in cognitive radio networks: Solutions and future research directions. In Proceedings of the IEEE

[2] Buchegger, S. &Boudec, L. (2002) Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland

[3] Dhurandher, S. K. &Mehra, V. (2009). Multi-path and message trust-based secure routing in ad hoc networks. In international conference advances in computing, control and telecomm. Technologies,

[4] Farruh Ishmanov, Sung Won Kim andSeungYeob Nam (2014). **A** Secure Trust Establishment Scheme for Wireless Sensor Networks.In proceedings of IEEE vol .98 no.12,pp 123-178.

[5] H.Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks", Journal Wireless Personal Communications: An International Journal archive, vol. 56, no. 3, (2011)February.

[6] Islam tharwat Abdel-Halim and Hossam Mahmoud Ahmed Fahmy, "Agent-based trusted on-demand routing protocol for mobile ad-hoc networks",Springer Science and Business Media New york (2014)

[7] Michiardi, P., &Molva, R. (2010) CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the 6th IFIP conference on security communications, and multimedia

[8] Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trustbased on-demand multipath routing in mobile ad hoc networks. Information Security, IET, 4(4), 212–232.

[9] Liu, K., & Deng, J. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5), 536–550. 2010.

[10] Pirzada, A. A., McDonald, C., &Datta, A. (2011). Dependable dynamic source routing without a trusted third party. Journal of Research and Practice in Information Technology, 39(1), 71–85.

[11] Papadimitratos, P., & Haas, Z. J. (2008) Secure routing for mobile ad hoc networks. In Proceedings of the SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), San Antonio, TX, pp. 27–31.

[12] Sun, Y. L., Yu, W., Han, Z., & Liu, K. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, 24(2), 305–317

[13] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications

[14] Yaserkhamayseh, Ruba Al-Salah, MuneerBaniYassein,(2012). **"**Malicious nodes detection in MANETS: Behavioural analysis approach" in Journal of Compuer Communications, vol 28(1)

[15] Y. Zhang, J. Mee Ng and C. Ping Low, "A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks", Journal of Computer Communications, vol. 32, **(**, pp. 189-202