Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

MQMF : Multiple Quality Measure Factors for Trust Computation and Security in MANET

By Kotari Sridevi & Dr. M. Sridhar
Muffakham Jah College of Engineering and Technology, India

Abstract- Identification of the mobile ad hoc network node in a secure, reliable communication is a very important factor. It will be a node in the service of reconciliation and node behaviour leads to uncertainty. It is always challenge to manage node security and resource due to the complexity of high mobility and resource constraints. Trust based security provides light-weight security computing for individual node trust to provide reliable and quality of service. In this paper we present a multiple quality measure factors (MQMF) approach for computing node trust to improvise the quality of service. It compute four quality measure factors based on node throughput and packet drop during communication to measure the node individual trustworthiness. It prevent the network from anomalous and malicious nodes to improvise the security and throughput. The evaluation measures shows an improvisation in throughput with less packet drop and computational overload in compare to existing protocols.

Keywords: *MANET, security, QOS, multiple quality measures, trust computation.*

GJCST-E Classification : *D.4.6, F.1.1*

Strictly as per the compliance and regulations of:

MQMF : Multiple Quality Measure Factors for Trust Computation and Security in MANET

Kotari Sridevi [α] & Dr. M. Sridhar [σ]

Abstract- Identification of the mobile ad hoc network node in a secure, reliable communication is a very important factor. It will be a node in the service of reconciliation and node behaviour leads to uncertainty. It is always challenge to manage node security and resource due to the complexity of high mobility and resource constraints. Trust based security provides light-weight security computing for individual node trust to provide reliable and quality of service. In this paper we present a multiple quality measure factors (MQMF) approach for computing node trust to improvise the quality of service. It compute four quality measure factors based on node throughput and packet drop during communication to measure the node individual trustworthiness. It prevent the network from anomalous and malicious nodes to improvise the security and throughput. The evaluation measures shows an improvisation in throughput with less packet drop and computational overload in compare to existing protocols.

Keywords: MANET, security, QOS, multiple quality measures, trust computation.

I. Introduction

Mobile ad hoc networks are self-organized and self-controlling wireless networks without infrastructure support. Due to the unavailability of any fixed prevention and security mechanism and centralized controlling and management system, an ad hoc network is facing major security issues and threats. It is a high challenging task to prevent ad hoc communication network form different attacks and intrusions. Even though many security protocols are proposed in this direction, but they all attained high overload due to the complexity in security mechansim. It requires a light-weight security protocol through which it will be able to provides a good quality of service and also prevent the node and network from attacks. The quality of service is reflected in the expectations and behaviour of the target node through a measures of its trust, honesty, availability, past and future activity. One of the nodes which are connected to each other on the relationship, reflecting the behaviour of a node which will be reflect by its trust, reliability, and trustworthiness [3],[7].

The network node provides the coordination between the nodes in the route protocol packets to route and rely on neighbourhood relationships [8]. To achieve a quality and secure performance standard a strong, stable and secure routing protocol is needed, which can maintain node link and mobility effectively. These effectiveness will be achieve the highest security and results against the aggressive nature of the environment. It also helps the nodes to form a secure cooperate link with other nodes and identifying the misbehaving network nodes that does not try to create instability [9]. The presence of misbehaving mainly carried out routing updates, or to advertise the wrong routing information and answer the old routing information from injecting false routing updates that make detection more difficult [1],[2].

In mobile ad hoc networks (MANET) trust-based security is an important feature. This enables organizations to deal with the uncertainty caused by the uncontrolled and open motivation to others [6]. Trust estimation and management are complex issues in MANETs due to the computational complexity of the issues and movements representing the most nodes [11], [16]. This prevents direct methods of other networks. In MANET, unreliable node can cause serious harm and adversely affect the quality and reliability of the data. Therefore, the trust and confidence level of the analysis of a node has to be positive impact on the trust with which the node conducts operation with the other node [5], [21]. In this paper, we present a protocol based on multiple quality measure factors (MQMF) to compute neighbour nodes trust and to achieve a quality and protected communication in mobile adhoc network. Mostly conventional schemes [10],[14],[19] proposed for ad hoc network trust computation have a high variation in realistic results [18]. This proposal provides a unified unit trust identification protocol enhances in MANETs security management node level of confidence and trust identity.

The rest of the paper is organized as follows. Section-2 presents the related work on trust based routing and security enhancement. In section-3, we present the proposed MQMF approach description and its mechanism. Section-4 describes the experiment and results evaluation and section-5 describes the conclusion of the paper.

II. Related Works

There are many related works performed in MANET for securing routing to achieve high quality throughput. It can be categorized in two different

Author α: Research Scholar, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India. e-mail: devijak@gmail.com
Authorσ: Associate Professor, Department of Computer Applications, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India.

category based on their securing mechanism for different type of attacks.

In the first category, the most common method used to create a security association between the source and destination in most on-demand routing protocols, such as DSR, DSDV and AODV to ensure security [22]. In [26], the authors proposed a proactive SRP, called SEAD, according DSDV using one-way hash chains to provide authentication for the attack and modify routing information broadcast and replay attacks. In [27], in order to ensure on-demand protocols such as AODV and DSR, the authors proposed an authenticated routing protocol, called ARAN with digital signatures to provide end-to-end authentication, message integrity, and nonrepudiation. In the second category, the main goal is to protect against internal attacks in the routing traffic. In [28], the authors proposed to use both path and message redundancy to detect behavioral state by comparing different copies of a message received on a different path. The accumulated path is protected by the accumulation of signature schemes [29], which is even more expensive than RSA signatures.

Trust have an attention to a number of areas of implementation towards secure system, and it also has a wireless network to gain importance as well [13], [17]. Each has its own disciplinary procedures of literature and it has a difficulty with the filters. Studies have recently been studied in many literatures, the security systems based on trust, identity-based methods are important in MANETs [15].

In [4] and [12] trust based on direct observation of the value of a trusted node is obtained using Bayesian methodology. Sun et al. [23] found to be working well, and the entropy values of trust by a trust model is used to evaluate and plan and direct observation of uncertainty in the case of the Trust. Trust based research compared with direct observation, indirect observation or second-hand information that may be important to assess the integrity of the node. For example, the collection of evidence from the neighboring nodes when not performing the quality of the other node in a situation that other people will detect of behavior.

Ariadne [20] protocol confirmed by a route using one of three procedure: a secret key between each pair of nodes, shared secret operation of end-to-end along with the broadcast authentication. But Ariadne will ensure that lie routing requests or replies do not get source or destination, where they did not know the node caused by forged or falsification.

Secure Routing Protocol (SRP) [24] is a route discovery protocol that moderate the unfavorable effects of misbehaving activities. This protocol assumes that the security relationship between any two nodes that want to communicate exists. The source and destination will be able to use cryptographic techniques to protect their relationship on the basis of the security associations. It requires a security check only between the source and destination of the route using the MAC RREQ and RREP packets. SRP does not implement any two nodes relay route request and route reply, which said protocol lightweight and insecure authentication to various attacks.

Security-aware ad hoc Routing (SAR) [25] protocol transforms AODV [22] routing protocol to include trust hierarchies with the incorporated nodes for path evaluation and selection. Protocol implements the trust level in the organizational hierarchy using share key in each level that each nodes can express their security requirements for the requested route and only nodes which meet the following requirements only will allow to participate in the route. However, as of the node trust, key distribution, knowledge of other key components are not addressed in this proposal work.

The level of trust in their approaches to the understanding of faith, measure and calculate that work in a variety of characteristics. Given the context of a node, the node trust, reliability and the accuracy of the information received from or traversing the node is a representative of the subjective evaluation. We tested the idea protocol in comparison with SAR [25] to evaluate the use of a MANET routing protocol and procedures for distribution of trust in identity important and promising approaches and routing mechanism in the following sections.

III. Multiple Quality Measure Factors Approach

The propsed MQMF approach performs its operation in three different stages as, Acquisition of CA certificates, computation of trust using MQMF factors, and MQMF based Trust Routing Mechanism. We assume that, both kind of internal and external attacks are present in the network, and all the node present in the network are considered as trustworthy. A secure identification key as *id_key,* for each node will be provided using a asymmetric cryptography mechanism in a network. This *id_key* is utilized to protectthe message fabrication through a message encryption.

a) Acquisition of CA Trusted Certificate

Acquisition of CA trusted certificate will be obtained from a trusted third party authority, before joining the network. This certificate is loaded one time and it remain in the node till it revoke. It validity remain for lifetime, but it become ineffective if the node trustworthiness degrades below the threshold level decided. The notations used in trusted certificates for a node Certificate representation as N_{CA_cert} are denoted as,

Notation	Description
$CA\_T_{pub\_key}$	Certificate authority Trusted Public Key
$CA\_T_{pvt\_key}$	Certificate authority Trusted Private Key

N_T_{key}	Node Trusted Key
N_{add}	Node Unique Address
N_{pub_key}	Node Public Key
N_{pvt_key}	Node Private Key

and, the certificate issued by a trusted CA is represented as,

$$N_{CA\_cert} = \boldsymbol{E}_{\boldsymbol{CA\_T_{pvt\_key}}}[N_{add}, N_{pub\_key}, CA\_T_{pub\_key}, E(N\_T_{key})_{N_{pvt\_key}}]$$

A trusted CA certificate provides a Public and Private key, which will be used for enccryption and decryption. Along with the CA key the certificate also provides, nodes address, it's public and private key, and a trusted key. All these are bundled and encrypted by node private key N_{pvt_key}, and the entire certificate is secured with CA private key, as $CA\_T_{pvt\_key}$. A node performs the verification of the other node by comparing their trusted CA public key, $CA\_T_{pub\_key}$ which is provided in the certificate.

b) Computation of Trust using MQMF factors

The proposed MQMF approach performs the trust computation as *T*, based on four factors as, *Correct_mf*, *Incorrect_mf*, *Lost_mf* and *Throughput_mf* rate. A *Correct_m ,as* C_{mf}, measures the node identity correctness being produced by a node during the verification, and an *Incorrect_mf as* I_{mf}, measures the rate of identity failure or wrongly produced the key for the verification. These two, C_{mf} and I_{mf} factors are being used for trust computation. *Lost_mf as* L_{mf}, calculates the data packets lost or dropped during communication, and *Throughput_mf* as T_{mf}, calculates number of data packets delivered. L_{mf} and T_{mf} factors are used for the quality measures computation. The equations for the calculation of C_{mf}, I_{mf}, L_{mf} *and* T_{mf} are shown below.

$$C_{mf} = \sum_{i=0}^{n} correct\_measure \qquad (1)$$

$$I_{mf} = \sum_{i=0}^{n} Incorrect\_measure \qquad (2)$$

$$L_{mf} = \sum_{i=0}^{d} lost\_pkts \qquad (3)$$

$$T_{mf} = \sum_{i=0}^{d} pkt\_delivered \qquad (4)$$

Where, *n* represents different iteration cycles performed for the node identification during communication cycle, and *d* represents the number of data packets communicated during the communication cycle.

Based on the above computation value of C_{mf}, I_{mf}, L_{mf} and T_{fmf} of a node, trust rate as NT_{rate} will be computed for each node using equation-5, and throughput rate as PD_{rate} will be computed for packet delivery using equation -6.

$$NT_{rate} = \frac{(C_{mf} - I_{mf})}{n} \times 100 \qquad (5)$$

$$PD_{rate} = \frac{(T_{mf} - L_{mf})}{d} \times 100 \qquad (6)$$

Using , NT_{rate} and PD_{rate} we will compute the final Trust Computation as $T_{measure}$ for each node to perform a trust decision during communication using equation-7. The runtime decision different trust threshold limit value will be considered for the evaluation of throughput. The following section discusses the routing mechanism using as $T_{measure}$.

$$T_{measure} = \frac{(NT_{rate} + PD_{rate})}{2} \qquad (7)$$

c) MQMF based Trust Routing Mechanism

All routing protocols objectives is to perform efficient routing in mobile adhoc network. In the initial stage generally routing protocol discover the routes to send data. But, in MQMF protocol, along with route discovery it also compute $T_{measure}$ for each node before sending data. In MQMF routing mechanism, we initially considered that all nodes are normal and trustworthy. The routing mechanism for the data routing is described in Alogrithm-1 using MQMF $T_{measure}$ which is computed using equation-7.

Algorithm 1: MQMF based Trust Routing Mechanism

Source node N init data forwarding → *forwardData* (D_{addr}, *Data*, *pkt_seqno*)

Method1: forwardData (Dest$_{addr}$, Data, sqno)

Trust_Threshold_limit = 25;

N gets the first hops nodes from the route table → $Node\_F_{hop}[]$

For "*p=0; p <= number of packet to send*" **Loop**
  For "*h=0, h<= number of hops*" **Loop**
    $Node\_F_{hop}[h]$ → *first_hop*
    Compute_NodeTrust_Rate (f_hop) → NT_{Rate}
    Compute_PacketDelivery_Rate(f_hop) → PD_{rate}
    Compute_Trust_Measure (NT_{Rate}, PD_{rate}) → $T_{measure}$

    if $T_{measure}$ >= *Trust_Threshold_limit* **then**
      forwardData → *first_hop*
    else
      Compute next forwarding hop $T_{measure}$ from $Node\_F_{hop}[]$
    end if
  End for
End for

Every intermediate node in the route verify the $T_{measure}$ of their next hop before forwarding data in the route. A source node initiates the data packets routing using the path discovered. Each node in the path verifies its neighbour node identity by producing a trust key, N_T_{key} which secured with encryption using $CA\_T_{pub\_key}$. On successful verification the node identity its *correct_measure* is incremented, in case of wrong identity its *incorrect_measure* is increased by 1. The identified neighboring node checks the $T_{measure}$ value of each firt hops node before passing up the data packets. The node sends the data packets to node which have the highest $T_{measure}$ value. This mechanism will guarantees the source the successful delivery of data packets through the trusted nodes. On successful delivered *pkt_delivered* is incremented, and in case if loss or drop *lost_pkts* is incremented by 1.

All intermediate nodes must send a signed confirmation of the previous hop for the delivery of a data packet to the next hop. If the next hop is not able to provide the confirmation to the intermediate node then it send an error the next hops. If an intermediate node on the path to the target jumps all else fails, send an error message to the source path. Source punishes all nodes in the path by reducing their $T_{measure}$ value, such that in the future such nodes can be avoided for the communication.

IV. Experiment Evaluation

a) Simulation Setup

To evaluate MQMF approach we modified the AODV protocol and evaluated the effect of our proposed protocol in comparison with SAR[25] and AODV[22] using Glomosim Simulator. The packet header size of route request and routing has increased as we added the security parameters. We simulate the simulation with the following setup parameters as described in Table-1.

Table 1 : Simulation Parameters

Configuration	Parameter Values
Simulation Area	1200m X 1200m
No. of Nodes	50
Mobility Speed	0 to 20 m/s
Source-Destination Pairs	20
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Mobility Speed (m/s)	0,20,40,60,80,100

The experiment analysis is perform using the parameter described in Table-1. The simulation evaluated for 600 seconds with varying the mobility speed from 0 to 100m/s in a Random Way-point model mobility. We consider mobility changes for the evaluation, as it have high impacts on the performance of throughput. For the security and for the trustworthiness measure evaluation we introduced 25% of malicious nodes.

During the route discovery all nodes in the network are normal and trustworthy, but during simulation a 25% of the malicious nodes are chosen dynamically to disrupt the network. These malicious node in network generally drop all the packets it receives and produce invalid identification during verification. However all of the data modification attacks can be detected using signature verification in MQMF approach and dropping of the financial data packets misbehaving by the network. For this evaluation we measured throughput and control overhead.

V. Results Evaluation

a) Throughput

Throughput is measure based on the total number of packet delivered against the total number of data packets originated. The evaluation of throughput result is presented in the absence and presence of malicious nodes.

Figure-1 and 2, presents the throughput performance comparison between the protocol. All protocol shows relatively drop of throughput with increasing of speed in both presence and absence of malicious nodes. The MQMF protocol shows an improvisation compared with AODV and SAR protocols in the presence of malicious nodes. The improvisation of the secure data throughput due to routing through a trusted node. In the absence of malicious illustrates the average performance due to the cryptography overhead. The proposed MQMF shows 25% improvisation in throughput and 10-20% downfall of throughput in presence of malicious nodes.

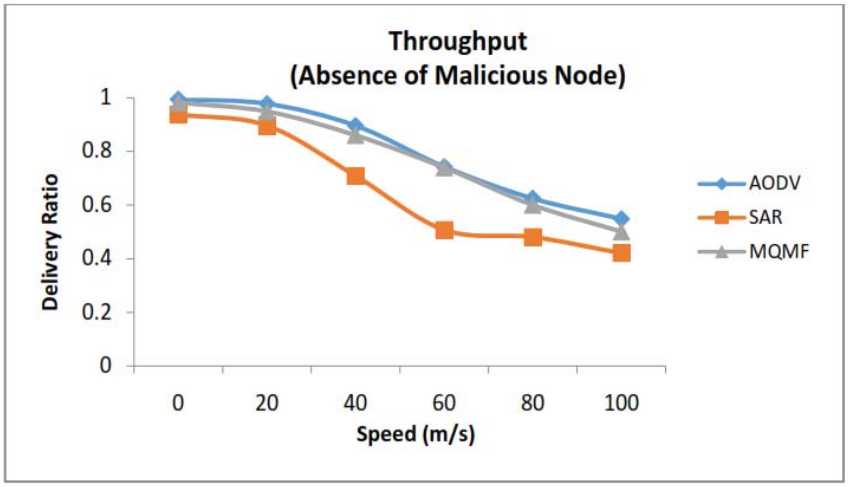

Figure 1 : Throughput in Absence of Malicious Nodes

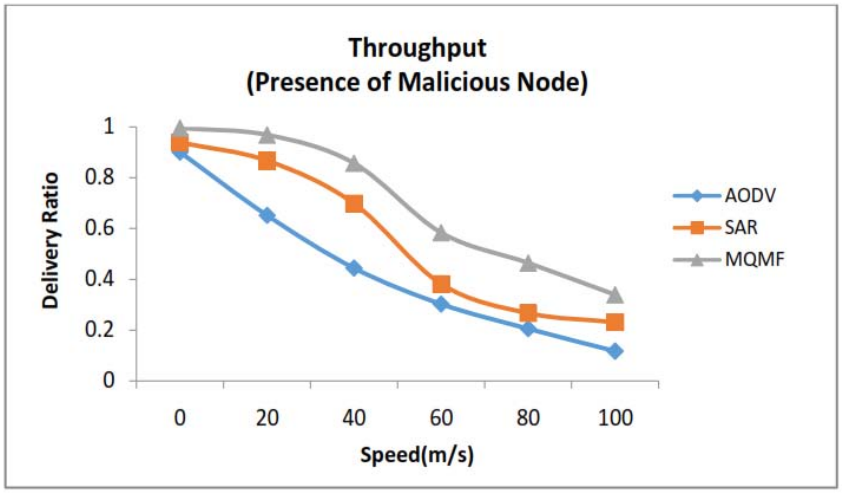

Figure 2 : Throughput in Presence of Malicious Nodes

b) Control Overhead

Control overhead measures the computational load over the network to perform the protocol execution. Its computed based on the total number of control packets exchanged during the complete communication cycle of the simulation.

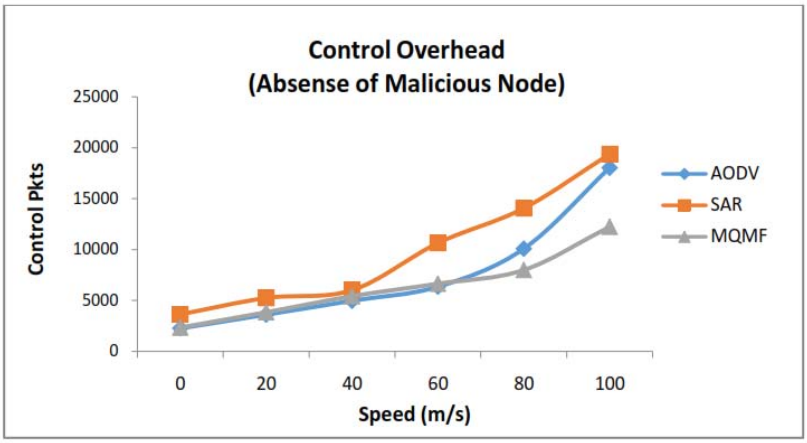

Figure 3 : Control Overhead in Absence of Malicious Nodes

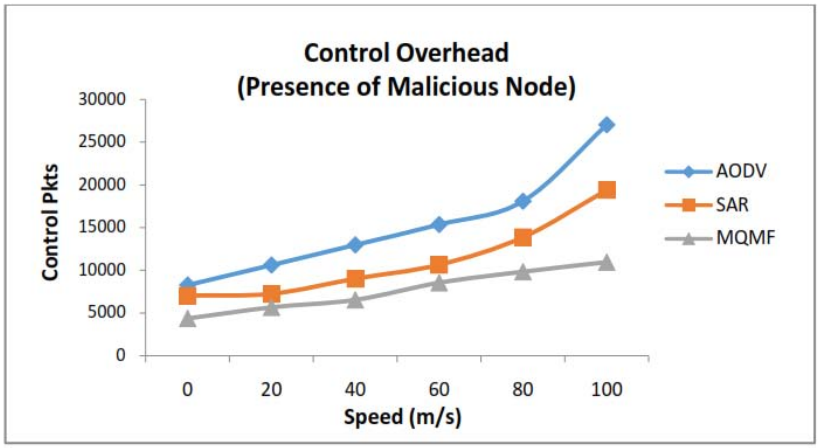

Figure 4 : Control Overhead in Presence of Malicious Nodes

Figure-3 and 4 shows control overhead in the absence and presence of malicious nodes between MQMF and other protocols. All protocol shows relatively increase in overhead with increasing of speed in both presence and absence of malicious nodes. MQMF shows low overhead incompares to others in presence of malicious nodes due to the trust computation and node identification which builds a secure path, where as SAR protocol carry out safety inspections repeatedly during communication and in AODV a lot of link failure with varying speed and the presence of a malicious node increases the high number of control packet exchange, which increases their routing overhead in compared with MQMF protocol.

c) *End-2-End Delay*

End-2-End delay evaluation measures the time taken by a data packets to reach the destination from source. The evaluation of our proposal in compare to AODV and SAR is presented in Figure-5 and 6 in the absence and presence of malicious nodes. In the case of absence of malicious node AODV performs superior in minimum speed but makes high delay in case high mobility in compared to SAR and MQMF. SAR and MQMF also shows an increase in delay with mobility speed due to more number link lost, but maintains low in compare AODV due to regular monitoring of their neighbour nodes. In case of presence of malicious node AODV suffers due to high no route loss due to malicious node and link failure due speed. But, MQMF and SAR mechanism identifies the low trust node effectively make them route data safely to the destination. In compare MQMF show low delay against SAR because MQMF $T_{measure}$ helps to dynamically route the data through trusted node which minimize the delay and improve the throughput and quality of service.

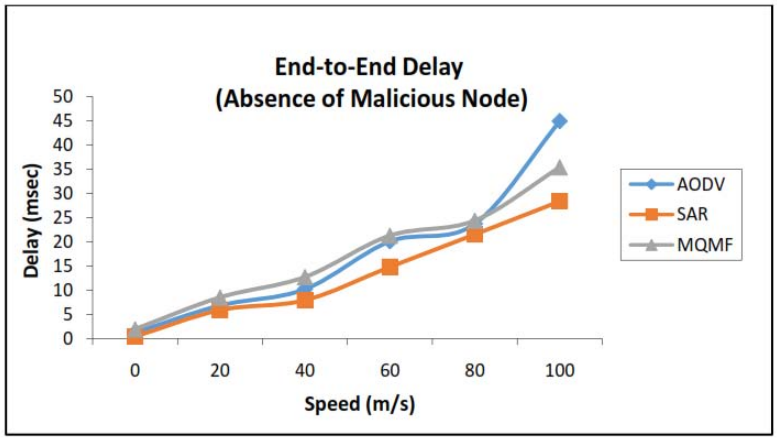

Figure 5 : End-2-End Delay in Presence of Malicious Nodes

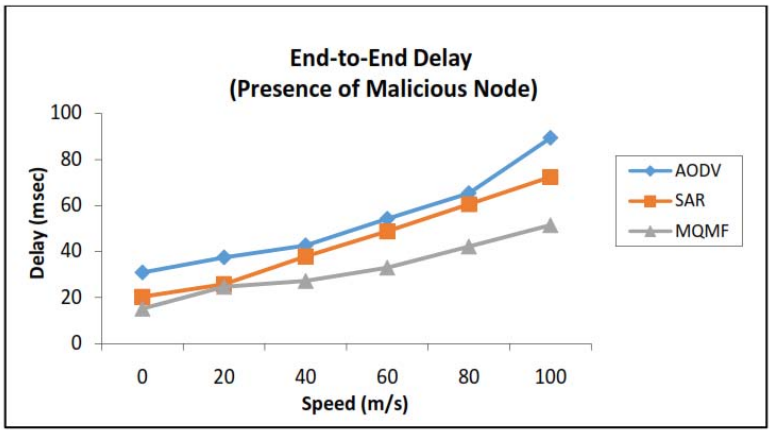

Figure 6 : End-2-End Delay in Presence of Malicious Nodes

VI. Conclusion

We proposed a new trust-based secure routing protocol as MQMF exclusive for mobile networks. MQMF authenticated routing node based on trust certificate and their hope is to identify the computer at the time of the communication. MQMF handle data routing through many paths to each destination. Every other node in the network store a local trust value and in the path table. This mechanism will guarantees the source the successful delivery of data packets through the trusted nodes. The simulation performed and compared with the performance of MQMF with AODV and SAR. MQMF achieves the similar throughput in compare to AODV and SAR in absence of no misbehaving nodes in the network, where as in the presence of misbehaving nodes MQMF shows an outperform over AODV and SAR in the throughput with a minimal overhead variation. In both cases, MQMF achieve high througput with establishing a reasonable network overload. The increase in the value of the trust for the period of time can lead to convergence. Also, a study to measure the effects of changes in that aspect of the protocol activities in the future are required.

References Références Referencias

1. Hui X., Zhiping J, Xin, Lei J, Edwin H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Elsevier, Vol-11 (n.d), p-2096-2114, 2013.
2. Ch En Xi, S Liang, MA JianFeng, MA Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", Network Technology And Application, China Communications, April 2015.
3. Z. Wei, H. Tang, F. Richard Yu, M. Wang and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.
4. Ing-Ray C., Jia G., Fenye B. ,Jin-Hee C., "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", Elsevier, p-59-74, 2014.
5. K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012.

6. Ming Li,S. Salinas, Pan Li, Jinyuan S., and X. Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence", IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015.
7. W. Liu and Ming Y., "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.
8. Changiz R., Halabian H., F.R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in cooperative wireless relaying networks," Wireless Commun. Mobile Comput., Sep. 2012
9. Yu F. R., Tang H., Bu S., and Zheng D., "Security and Quality of Service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J. Wireless Commun. Netw., vol. 2013, pp. 188-190, Jul. 2013.
10. Sarvanko H., Hyhty M., Katz M. and Fitzek F., "Distributed resources in wireless networks: Discovery and cooperative uses," in 4th ERCIM eMobility Workshop in conjunction with WWIC'10, 2010.
11. J. Lopez, R. Roman, I. Agudo, and C. F. Gago, "Trust management systems for wireless sensor networks: Best practices", Computer. Communication. vol. 33, no. 9, pp. 1086-1093, 2010.
12. H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor neworks," in Proc. IEEE GLOBECOM Workshop,pp. 153-157, Dec-2010.
13. J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tuts., vol. 13, no. 4, pp. 562-583, Fourth Quarter, 2011.
14. M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol," in International Symposium on Trusted Computing and Communications, Trustcom, pp. 802-808, 2009.
15. S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 3, pp. 1025-1036, Mar. 2011.
16. Xia H., JiaZ.,Ju L, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules", in Proc. IEEE/ACM Green Computer Communication., 2011.
17. J. Hassan, H. Sirisena, and B. Landfeldt, "Trust-based fast authentication for multiowner wireless networks," IEEE Trans. Mobile Comput., vol. 7, no. 2, pp. 247-261, 2008.
18. Q. Nguyen, L. Lamont and P. C. Mason, "On trust evaluation in mobile ad hoc networks," Security and privacy in mobile information and communication systems, Springer, vol. 17, pp. 1-13, 2009.
19. Boukerch A., L. Xu and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Computer Communications, no. 30, pp. 2413-2427, 2007.
20. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Wireless Networks, 11(1-2):21-38, 2005.
21. L. Kagal, T. Finin and A. Joshi, "Trust-based security in pervasive computing environments," IEEE Computer, vol. 34, pp. 154-157, 2001.
22. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.
23. Sun .Y,W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305-317, Feb. 2006.
24. Z. Haas and P. Papadimitratos, "Secure routing for mobile ad hoc networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), Jan. 2002.
25. S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad-hoc routing for wireless networks", In MobiHOC Poster Session, 2001.
26. Y.C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", In Proc. 4th IEEE Workshop Mobile Computing Syst. Applications, June 2002.
27. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. BeldingRoyer, "Authenticated routing for ad hoc networks", IEEE Journal Selective Areas Communincation, Vol. 2, No. 1, Mar. 2005.
28. M. Yu, S. Kulkarni, and P. Lau, "A new secure routing protocol to defend Byzantine attacks for ad hoc networks",In Proc. IEEE Int. Conf. Networks (ICON'05), vol. 2, pp. 1126-1131, Nov. 2005, Kuala Lumpur, Malaysia.
29. D. Boneh, C. Gentry, H. Shacham, and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps", in Proc. Advances in Cryptology - Eurocrypt-03, LNCS, 2003.