Providing Security for MANETs using Hybrid Trust Mechanism

Taha Naheed*[1],C.Atheeq[2],Dr.SyedRaziuddin[3]
Student*[1] ,Assistant Professor[2],Professor[3]
Department of CSE*[1] ,
Osmania University[1], Hyderabad, India

Abstract : A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. For quick data transmission, we need a routing protocol that adapts to topology changes. In the open, collaborative MANET environment, practically any node can maliciously or selfishly disrupt and deny communication of other nodes. In MANET secure data transmission is one of the best issue. We are doing enhancement in the secure data transmission in MANET using trust based multipath routing protocols. We are plotting graph of trust based secure data transmission with existing system by consideration factors Packet delivery ratio, End to end packet delay, Throughput.

***IndexTerms*-Manets,trust computation,throughput,security**

I. Introduction

In this period of computing, the interest for Wireless Local Area Networks has developed remarkably. The desire for this sort of computing was made reasonable with the appearance of IEEE 802.11 [1] and it soon turned into an accepted standard for the WLANs. This prompted the acknowledgment of an idea that really supports the anywhere and anytime computing, called as Infrastructure less remote systems. A Mobile Ad hoc Network (MANET) is an Infrastructure less remote system. A MANET is composed of stations that communicate with each other directly in a peer-to-peer fashion. Thus, an ad hoc network is independent of any existing network infrastructure, such as base stations and access points. Examples of simple ad hoc networks are two mobile phones connected through Bluetooth or two laptops connected through IEEE 802.11 (operating in ad hoc mode).

Mobile Ad Hoc Networks (MANETs) are having the capacity to end up noticeably the key parts in the 4G engineering. Mobile ad hoc networks are formed dynamically by a set of autonomous mobile nodes that are connected via wireless links without using a network infrastructure or centralized administration. The nodes can move uninhibitedly and sort out themselves haphazardly. In this way, the system's remote topology may change quickly and unpredictably. Such a system may work in a standalone fashion or might be associated with the bigger Internet. Routes between nodes in a ad hoc network may incorporate multiple hops [2] because of the way that nodes fill in as both hosts and routers. Figure 1.1 demonstrates a mobile ad hoc network. The communication topology is also shown in the figure

Fig 1:A Mobile Adhoc Network

As appeared in Figure 1.1, an ad hoc network may comprise of home-processing gadgets including note pads, handheld PCs, and so forth. Each node can communicate with different nodes that reside within its transmission run. For communicating with nodes that reside past this range, the node needs to utilize intermediate nodes to relay messages hop by hop [2]. Henceforth, some of the time MANETs are otherwise called multi-hop wireless network.

The security dangers of the integrated internet and manet could genuinely influence the execution of the integration strategy. The threats might have source in the ad hoc network or might additionally begin from the Internet. Also these attacks need variable way as far as aggravation they make in the network operations.Nodes might act maliciously because of distinctive particular circumstances whichever eagerness or unintentionally. A pernicious node resorts to black hole attack when it drops the packets without sending them to the next hop due to selfishness.It could be allowed that a node drops packets when it will be over-burden. The previous is a

occurrence of pernicious conduct inasmuch as last demonstrates that the node may be compelled on drop those packets because of congestion.

The remaining part of the paper is organized as follows:section2 makes the literature survey/Related work,section 3 explains the proposed system and results are presented in section 4 section 5 concludes the paper

II Related Work

Trust has been extensively studied in various other research domains, such as sociology, psychology, management, political science, philosophy, law and economics. In information technology, trust metrics and trust evaluation are mainly defined for public key authentication [2,3], access control [8] and electronic commerce[10]. However, all these schemes are proposed for static networks and thus cannot be applied directly in dynamic MANETs. With more and more research interests in security of MANET in recent years, some trust models designed for MANET have began to appear in literature. Ngai, Lyu and Chin [10] proposed an authentication service against dishonest nodes in MANEMT, by applying Beth, Borcherding and Klein's trust evaluation model designed in [11].

In Beth, Borcherding and Klein's approach, two types of trust are measured: direct trust and recommendation trust. Each type of the trust can be expressed and computed into a certain real number between 0 and 1 However, their approach is designed for open static networks. Its trust evaluation between two end nodes is based on either their direct experience or recommendation through others, but not both at same time for the two end nodes. So no relationship is defined to balance the direct trust and recommendation trust in their approach. Pirzada and McDonald [12, 14] proposed a trust model to establish trust in pure MANETs. The trust computation is based on monitoring data delivery in the network. The trust value is represented with a continuous range from -1 to +1. Negative value for trust can occur as a result of more failures than success for various events such as data forwarded, data received, control packets forwarded and etc. However, this model is designed for routing in MANETs. Their trust evaluation is solely based upon direct data communication of each node in MANETs. Neither recommendation from other nodes nor pre-existing knowledge among the node is considered.

Yan, Zhang and Virtanen [15] proposed a trust model for secure routing evaluation in MANET. The authors defined a large trust evaluation matrix based on statistic data collected during the network communication. The statistic fields try to include different affective factors of the evaluation, such as pre-existing relationship among the nodes. A linear function is proposed to link these statistic fields together to compute the trust value about a certain node or nodes. However, no boundary evaluation value is defined in their approach. So it is difficult to define a threshold trust value for ongoing tasks. Virendra, et al. [16] proposed a pair-wise trust evaluation scheme in MANETs. To evaluate the trustworthiness of a target node, a node implements some self evaluation on the target node while also considering other nodes' trust on the same target node. All trusts are evaluated via node monitoring on data delivery in the network. For computing self evaluation a traffic statistic function is mentioned, but not explicitly presented.

To combine the self evaluation and others' trust, a relationship equation is defined. In the equation, self evaluation and others trust are weighted with factor a1 and a2 respectively (a1+a2=1). The limitation of such relationship equation is that all different direct experiences are adjusted with one weight factor of same value. Meanwhile, it is not clear how to determine the value of a1 and a2. From the above review, we can see that each of the mentioned schemes has some limitations. Most of them implement trust evaluation by monitoring data delivery of the target nodes. Such approaches are suitable to routing trust evaluation, but not sufficient for node authentication in MANETs.

III Proposed System

In our trust model, we evaluate two types of trust between a trustor node and a trustee node: direct trust and recommendation trust. Direct trust is a kind of credential gained by a trustor node through its direct experience upon the trustee node. Recommendation trust is the credential gained by a trustor node from a third node or nodes' recommendation on the trustee node.

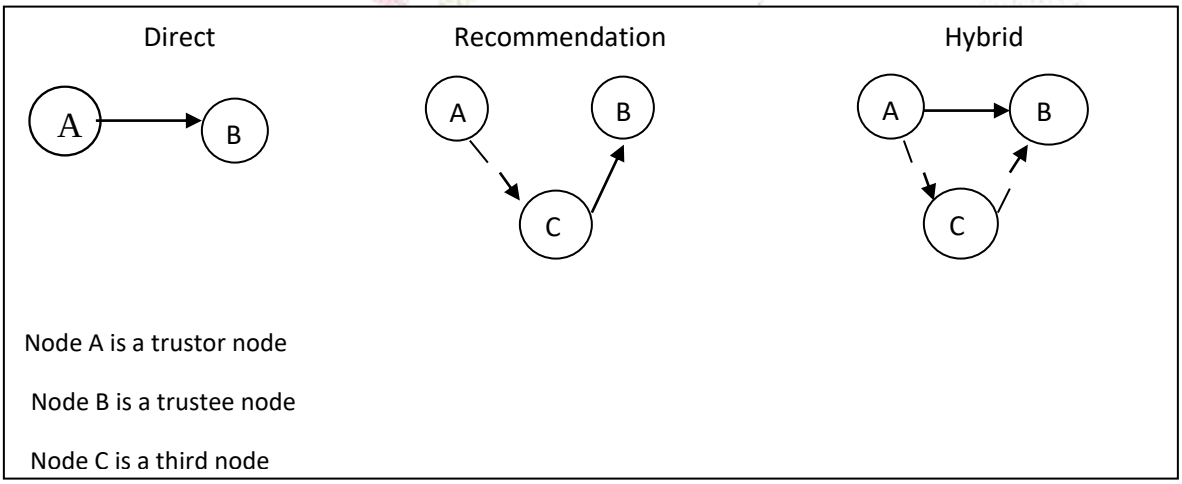

Fig:Trust Computation

Direct trust is evaluated basing on the direct experience that a trustor node may have on a trustee node. Such that it can be positive or negative. When a trustor node doesn't have enough direct experience on a trustee node, the trustor node may enquire to a third node for recommendation. To minimize the disadvantages of direct and indirect strategies, we will combine the methods i.e., a hybrid method

The idea of "Trust" initially gets from sociologies and is characterized as the level of subjective conviction about the practices of a specific entity18. So in order to have better communication between mobile node and a fixed node, we are finding the trusted nodes so that the data can be protected from malicious nodes.

The effective trust is calculated for the trusted nodes using hybrid method which is obtained by direct observation and recommendation based methods .The direct trust value[(DT$\sum_{x,y}$) of node x on y is obtained by

$$DT_{x,y} = W(R_p).R_p + W(R_q).R_q + W(R_e).R_e \quad (1)$$

Where W( ) is an assigned weight to event, ,,are optimized route reply misbehavior factor, route request misbehavior factor, route error misbehavior factor respectively. The values of R_p, R_q, R_e can be determined as

$$R_p = \frac{R_{ps}-R_{pf}}{R_{ps}+R_{pf}}; R_q = \frac{R_{qs}-R_{qf}}{R_{qs}+R_{qf}}; R_e = \frac{R_{es}-R_{ef}}{R_{es}+R_{ef}} \quad (2)$$

Where are the successful route reply acknowledgement packets, successful route request acknowledgement packets and successful route error acknowledgement packets respectively. Similarly are the numbers of failed packet.

The recommended trust value (RT $\sum_{x,y}$) of node x on y is obtained by the recommendation of third node z as shown in figure

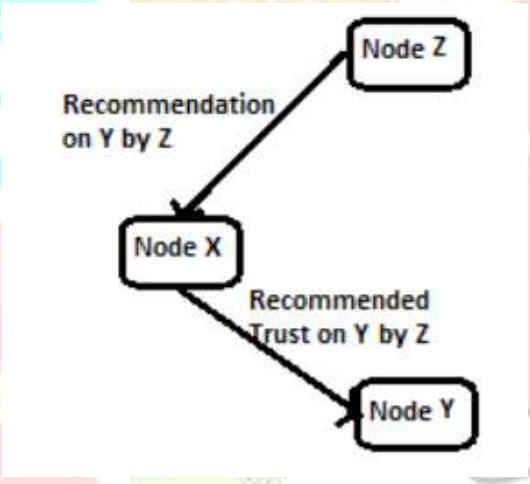

Figure 3. Recommendation based indirect trust establishment.

Now the effective trust value is evaluated through hybrid method

E=(αD+βR)/2 (3)

where α and β are constants such that α + β=1

IV Results

The proposed model is developed using NS2.34 & examined the overall performance of proposed model by comparing with the existing models. We evaluated the overhead of proposed model with respect to key size variation in mobile nodes of MANETs

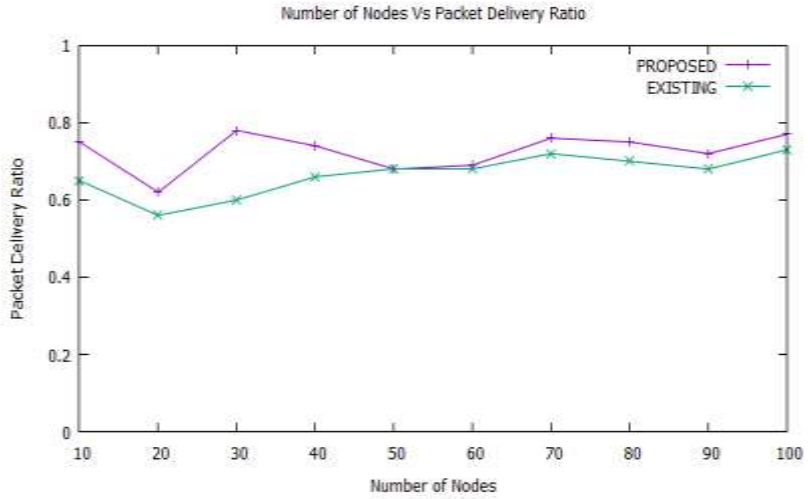

Fig 4: Comparision between Number of nodes Vs Packet Delivery Ratio

The above figure 4 represents the Number of nodes and Packet Delivery Ratio.The result shows that Packet delivery ratio increases in our proposed system when compared to existing system.

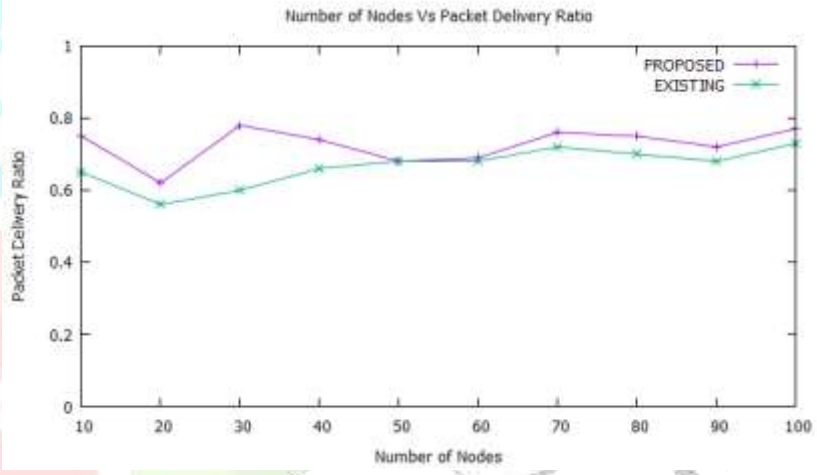

Fig5:Comparision between Number of nodes Vs Throughput

The above fig5 we are measuring the throughput of the network.The result shows that the throughputof the proposed system is more than the existing system.Thus the proposed system gives best results than the existing system.

Conclusion

In this paper we analyzed and surveyed many schemes in MANET for providing the trust to ensure in multiple perspectives .Due to its open nature it is difficult to maintain the trust and resource constraints, hence the trust is the desired challenge for best performance. This survey analyses all the possible trust management for secure routing in MANETs. The trust to be computed and social communities makes use of it to validate the measurements of a trust. This is very desirable in dynamic topology allocated to networks, such as MILITARY but with certain constraints like maintaining reliability, scalability, reconfigurability

References

[1].Dewan, P. and P. Dasgupta. Trusting Routers and Relays in Ad hoc Networks. in Proceedings of First International Workshop on Wireless Security and Privacy (WiSr 2003) in conjunction with IEEE 2003 International Conference on Parallel Processing Workshops(ICPP). 2003. Kahosiung, Taiwan: IEEE.

[2].Reiter, M.K. and S.G. Stubblebine, Resilient authentication using path independence. IEEE Transactions on Computers, 1998. v 47(n 12).

[3].Maurer, U., Modelling a Public-Key Infrastructure. Lecture Notes in Computer Science,Spring-Verlag 1996.v 1146:p.325.

[4] Atheeq, C. and Rabbani, M., 2017. Secure Intelligence Algorithm for Data Transmission In Integrated Internet MANET. International Journal of Computer Science & Applications, 14(2).

[5]. Josang, A. An Algebra for Assessing Trust in Certification Chains. in Proceedings 1999

Network and Distributed System Security Symposium. 1999. Reston, VA, USA: InternetSociety.
[6] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology, 9(26).
[7]. Zimmermann, P.R., The Official PGP User's Guide. 1995: MIT Press.
[8]. Herzberg, A., Y. Mass, and J. Michaeli. Access control meets public key infrastructure, or: assigning roles to strangers. in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 2000. Berkeley, CA, USA: IEEE.
[9]. Manchala, D.W. Trust Metrics, Models and Protocols for Electronic Commerce Transactions. in Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No.98CB36183). 1998. Los Alamitos, CA, USA: IEEE Computer Society.
[10]. Manchala, D.W., E-commerce trust metrics and models. IEEE Internet Computing, IEEE 2000. 4(n2): p. p 36-44.
[11]. Beth, T., M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. in 3rd European Symposium on Research in Computer Security (ESORICS '94). 1994. Brighton, UK: Springer Verlag.
[12]. Pirzada, A.A. and C. McDonald. Trusted Route Discovery with TORA Protocol. in the Second Annual Conference on Communication Networks and Services Research (CNSR'04). 2004. Fredericton, N.B., Canada: IEEE.
[13] Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. Indian Journal of Science and Technology, 9(47).
[14]. Pirzada, A.A. and C. McDonald. Establishing trust in pure ad-hoc networks. in Proceedings of the 27th conference on Australasian computer science. 2004. Dunedin, New Zealand: Australian Computer Society.
[15]. Yan, Z., P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solution in Ad Hoc Networks. in Proceedings of the Seventh Nordic Workshop on Secure IT Systems 2003.Norway
[16]. Virendra, M., et al. Quantifying Trust in Mobile Ad-Hoc Networks. in International Conference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05).2005. Waltham, Massachusetts, USA: IEEE.
[17]. Grandison, T.W.A., Trust Management for Internet Applications, in Department of Computing. 2003, University of London: London, British. p. 252.
[18] Atheeq, C. and Rabbani, M.M.A., 2017. Mutually authenticated key agreement protocol based on chaos theory in integration of internet and MANET.International Journal of Computer Applications in Technology, 56(4), pp.309-318.
[19] Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on (pp. 421-425). IEEE.