International Journal For Technological Research In Engineering
Volume 4, Issue 8, April-2017 *ISSN (Online): 2347 - 4718*

BEHAVIOUR BASED VOTING TECHNIQUE TO FIND OUT MALICIOUS BEHAVIOUR IN MANET

Himangri Singhal[1], Er. Hitesh Madan[2]
Department of Master of technology, Computer science, SRGI JHANSI, Uttarpradesh

Abstract: MANET is one of the most popular network technologies. The wireless connectivity and mobility of network devices enable it work in a number of applications. The network is not containing an incorporated control therefore the topology control is responsibility of routing protocols. In this way the routing protocols are dealing with the topology advancement furthermore in charge of course revelation and route administration. On the other hand due to absence of centralized control the network is suffers from the issues of security and performance. In this exhibited work the principle center is given on the execution change of the MANET. Thus a number of research articles are investigated where a number of recently developed techniques for refining the performance are available. But most of them are increases either controls message exchange or computationally expensive by which the end to end delay is affected.

Keywords: Manet ,AODV, Trust on manet, Internal attacks, External attacks.

I. INTRODUCTION

Wireless technologies such as Bluetooth or the 802.11 standards enable mobile devices to establish a Mobile Ad-hoc Network (MANET) by connecting dynamically through the wireless medium without any centralised structure . MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets , this multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions[1].

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes and connected in dynamic manner. Nodes forming a temporary/short-lived network without any fixed infrastructure where all nodes are free to move about arbitrarily. Nodes must behave as routers, take part in discovery and maintenance of routes to other nodes in the network. Wireless links in MANET are highly error prone and can go down frequently due to mobility of nodes. Stable routing is a very critical task due to highly dynamic environment in Mobile Ad-hoc Network[2].

II. AODV

AODV (Ad - hoc On – demand Distance Vector) protocol is a reactive or on - demand routing protocol. It does not maintain all the routes in the network, but it provide quick and efficient route establishment or discovery when they are needed thus it provides communication between nodes with minimal control overhead. The route is maintained between two nodes as long as it is needed. It provides loop free routing due to the use of destination sequence number, which is generated by the destination itself. If two similar routes to a destination exist then the node chooses the one with the highest sequence number. AODV is able to provide both unicast and multicast routing. It uses routing tables to store the routing information. like destination IP address, next hop IP address, destination sequence number, active neighbours for route and expiration time for the route. Expiration time is also called as the lifetime, which is reset each time when route has been used. If the lifetime is over then the route is considered as the invalid. AODV does not place any additional overhead on data packets because it does not use source routing. The major and critical steps involved in the algorithm used by AODV are route discovery and route maintenance[3]. AODV stand for Ad-hoc On-Demand Distance Vector Routing .AODV is meaning that it establishes a route to a destination only on demand.AODV is capable of both unicast, broadcast and multicast routing.AODV have some join feature of DSR and AODV.AODV avoids the countingto-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV reacts relatively quickly to the topological changes in the network and updating only the hosts that may be affected by the change, using the RREQ message. Hello messages, be dependable for the route maintenance, are also imperfect so that they do not create unnecessary overhead in the network. The RREQ and RREP messages are responsible for the route discovery[4].

III. TRUST ON MANET

A standard definition considers trust to be a measure of subjective belief that one person or party uses to assess the chance another can perform a good action before the chance presents itself to observe whether or not that activity has occurred. Once an individual is taken into account trustworthy, it's meant that there's a high chance that the actions they're expected to perform are done in a way that's

favorable to the trusted. In MANET trust will be outlined as a level of belief in line with the behavior of nodes the chance value of trust variable from zero to one wherever zero represents DISTRUST and one represents TRUST. Providing trust model in ad hoc networks is important as a result of it gains higher security level and improves efficiency within the network. The dynamics of this has contributed to three main analysis areas within the field of Trust Management for distributed ad-hoc networks. This includes work targeting Trust Propagation, Trust Aggregation and Trust Prediction [5]. Attacks on network come in many varieties and they can be grouped based on different characteristics. Many researcher used different aspect to classified the attacks on MANET classified the attack based on the trustworthiness of communication partner in the network. They divided the attacks on MANET into two main catagories by their sources, external attacks and internal attacks.

External attacks

The attacks are committed by the nodes that are not legally part of the network. The attackers are necessary to compromise one node in the target network. The target nodes might be a self-sufficient node that link to entire network using the same infrastructure or communication link. The compromised node would be use to initiate attack in the target network without even being authenticated. All network communication in the target network will be possible to break down by the attacker from outside through the compromised node. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on.

Internal attacks

Internal attacks are typically more severe attacks, the source of attacks are come from inside a particular network. A malicious inside node already belong to the network as an authorized party. A malicious node with access to all nodes in its range might pose a crucial threat to the capability of the whole network. Since the internal attacks are not easy to prevent, the attacks can be performed more efficiently. Moreover, the malicious nodes that is part of the network which assumed to be trusted by entire nodes might be use the standard security means to actually protect their attacks[6].

IV. LITRETURE SURVEY

Abrar Omar Alkhamisi (2016) et al. The proposed TSAOMDV aims at identifying and isolating the attacks such as flooding, black hole, and gray hole attacks in MANET. With the help of Intrusion Detection System (IDS) and trust-based routing, attack identification and isolation are carried out in two phases of routing such as route discovery and data forwarding phase. IDS facilitates complete routing security by observing both control packets and data packets that are involved in the route identification and the data forwarding phases. To improve the routing performance, the IDS integrates the measured statistics into the AOMDV routing protocol for the detection of attackers. This facilitates the TS-AOMDV to provide better routing performance and security in MANET. Finally, the Trust based Secured AOMDV, TS-AOMDV is compared with the existing AOMDV through the NS2 based simulation model[7].

David Airehrour, (2015) et al. this paper proposes, GradeTrust, a secure routing protocol for MANETs based on the trust levels of network nodes. It uses trust to isolate black hole routing attacks thus offering secure routing of data traffic as well as improved packet delivery ratio. Preliminary simulation results have shown that trust compromise and packet delivery ratio is better in GradeTrust compared to traditional routing protocols, such as AODV and FSR. Trust-based secure routing in MANETs has attracted lot of research attention worldwide. It is effective in providing secure routing by isolating malicious nodes and other overheads from MANETs[8].

Dr. Zeinab Movahedi, et. al. (2015) in this paper propose a taxonomy of main identified trust-distortion attacks based on how the trustworthiness estimation of a node about another node is distorted. In this paper, provide a holistic classification of main evaluation metrics which can be used to evaluate and compare such frameworks. For each framework, a unified approach is used to describe the trust model, taking each component required for trust management as a guideline. Moreover, each framework is analyzed regarding its resistance against different trust-distortion attacks, the framework unique features, merits, demerits and findings. Finally, Different trust-distortion resistant frameworks and outline the open issues and future research directions are compare[9].

Meenakshi Dubey et. al. (2015) In this paper, design reputation base trust allocation system for the node and if any fault occurs in any of the node. The particular node identify using node packet delivery ratio base analysis, in that technique it will calculate node packet delivery ratio of each node which will participate in the route and get node packet delivery ratio in less than certain limit that means node is faulty and will search for new route using Location Aided Routing (LAR). Above work behavior is analyzed through Network Simulator-2 test based architecture and also identifies the node trust level and faulty node as well as performance impact of AODV-Trust as well as AODV-LAR-Trust approach[10].

Muhammad Saleem Khan et. al. (2015) In this paper, first investigate the impact of trust update frequency on energy consumption and packet loss rate. |Then identify network parameters, such as packet transmission rate, packet loss rate, remaining node energy, and rate of link changes, and leverage these parameters to design an Adaptive Trust Update Frequency scheme that takes into account runtime network conditions. The evaluation of our prototype shows significant improvements in the tradeoff between energy saving and packet loss rate over traditional fixed-frequency approaches[11].

Kefayat Ullah et. al. (2015) in this paper propose a trust computation metric based on node's impulsive behavior to become malicious in dynamic scenario and proposed algorithms for trust evaluation of every node. Here it proposed a trust based security model (TSRM) for authenticating the new nodes as well as the nodes which are active in current communication network. TSRM captures

the evidence of trust worthiness for other nodes from the security model and in return assists them to make better security decision[12].

SJ. Indhu Lekha1, et. al. (2014) In this paper, it propose a Vectorbased trust mechanism (VBM) which nominates a CH based on the higher trust value computation with earliest bit vectors and Enhanced Certificate Revocation scheme (ECR) for discarding the authorization of the misbehaving nodes. This paper achieves greater reliability, consumes less energy, avoids false accusation, quicker revocation time, efficient trust value computation, also reduces the communication and computational costs compared to the existing mechanisms. Our simulation results expresses that the proposed mechanism yields an exemplary outcome for providing secure transmission in MANETs[13].

Heena1,et. al. (2014) In mobile ad-hoc network (MANET) environment, main task is to determine a suitable route among source and destination node such that delivery of the message can be guaranteed. The route should be picked in such a way so that whole nodes in the path are trustworthy, non malicious, non-selfish and with less hop count. Selfish nodes may not follow the collaboration pattern and cause a deliberate reduction in the performance of network. This paper detects a path among source and destination node which contains non-selfish, trustworthy nodes and try to keep less hop count[14].

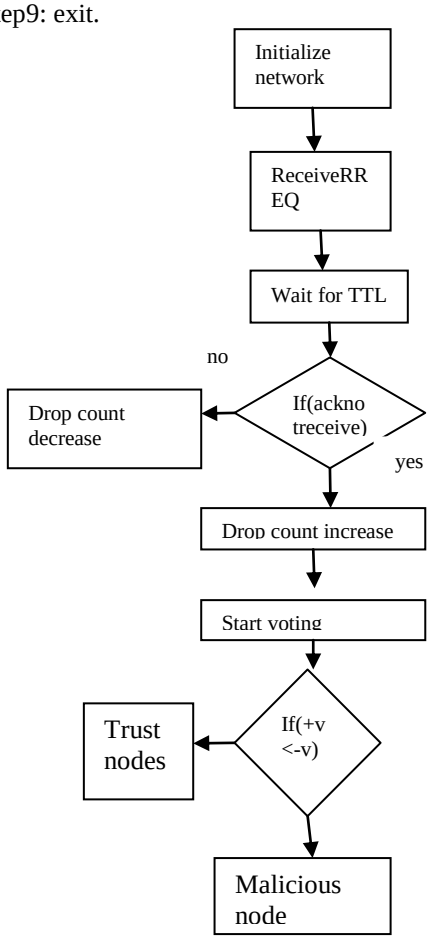
Hui Xia1, et. al. (2014) In this study, we abstract a basic decentralized effective trust inference model based on node's behavior assessment, where each peer assigns a trust value for a set of peers of interest. In this model, we introduce the 'voting' mechanism to access the recommending experience (or ratings), in order to reduce the cost of the algorithm design and the system overhead. Then combined with this trust model, a novel trust-enhanced multicast routing protocol (TeMR) is proposed. This new protocol introduces the group-shared tree strategy, which establishes more efficient multicast routes since it uses 'trust' factor to improve the efficiency and robustness of the forwarding tree. Moreover, it provides a flexible and feasible approach in routing decision making with trust constraint and malicious node detection[15].

V. PROPOSED WORK

Mobile ad-hoc network is most popular network now a days there are lots of work done regarding in this field security is a main concern of mobile ad-hoc network because of its infrastructure less property. In existing technique author did not mention any exact technique to calculate trust of nodes. so that there is no procedure of find out true node in network to overcome this problem we propose a packet drop based model to find out true nodes in network. In our proposed work first route request generate by source node to find out destination nodes after that malicious node generate fake route reply with shortest path, now source node send data to this node and this malicious node drop whole data after that source node wait for TTL and send data again with increment the drop counter of path node which send fresh sequence number now we check drop counter with thresh hold value if drop counter is greater than thresh hold source node broadcast malicious node id whole over network so all node compare drop count for this node and after that on the basis of drop packet voting node declare as malicious node.

algorithm

step1: initialize network
step2: generate RREQ
step3: receive RREP
step4:wait for TTL
step5: if(acknotreceive){
dropcount++
step6: if(dropcount>thershhold){
send node id to all nodes}
step7: voting start
step8: if(+vot<-vot){
node declare as malicious node
else
true node
step9: exit.



Simulation and result

Simulation of work done on ns-2.35 where for communication we take AODV routing protocol

Tool	Ns-2.35
Routing protocol	AODV
Anteena	Omni
Queue	Droptail
Mac	802_11
Buffer size	50
Stop	100
Type	Tworay

Packet delivery ratio:

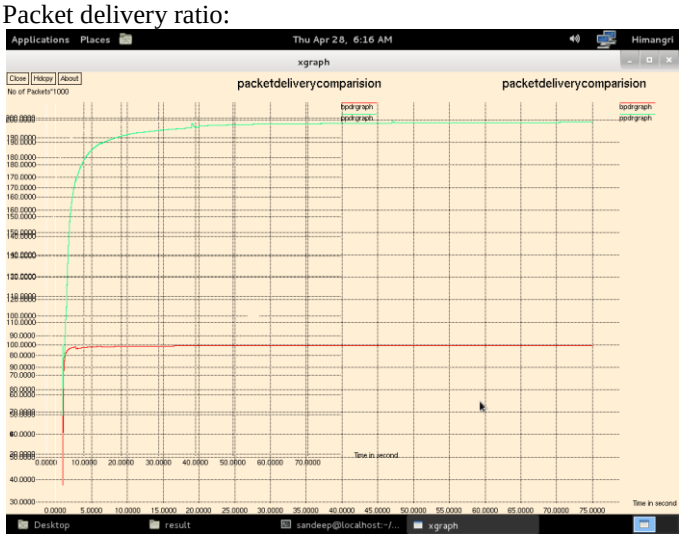


Fig: packet delivery ratio

Throughput:

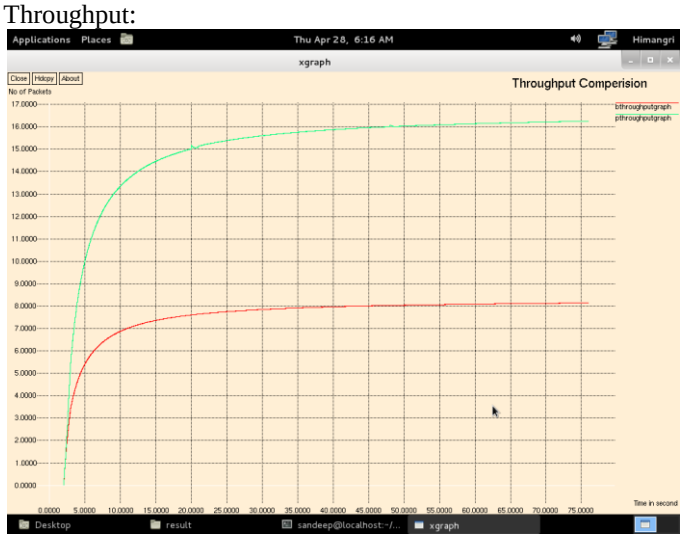


Fig: throughput

Routing overheD

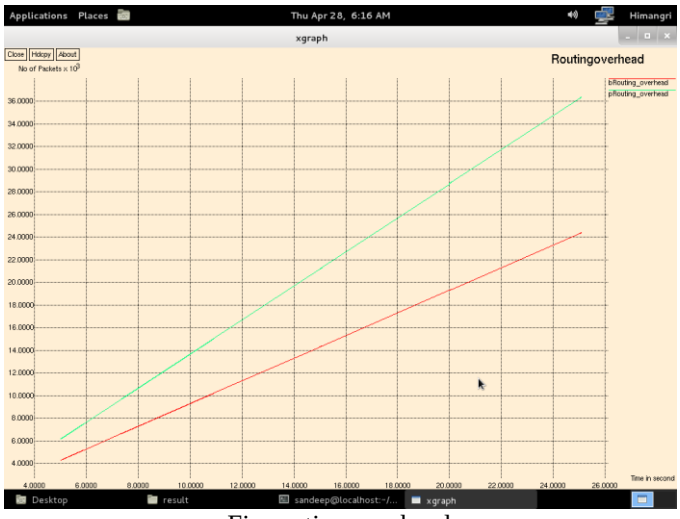


Fig routing overhead

Conclusion

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[2] Gurpinder Singh, Asst. Prof. Jaswinder Singh, "MANET: Issues and Behavior Analysis of Routing Protocols", Volume 2, Issue 4, April 2012, IJARCSSE.

[3] Daxesh N. Patel, Sejal B. Patel, Hemangi R., Rutvij H. Jhaveri, "A Survey of Reactive Routing Protocols in MANET", International Conference on Information Communication & Embedded Systems (ICICES 2014).

[4] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala, " A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", Harjeet Kaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 498-500.

[5] Mrs. S. Geetha, Dr. G. Geetha Ramani, "Survey of Trust Based Routing Protocols in MANET", Volume 4, Issue 10, October 2014.

[6] Nimitr Suanmali, Kamalrulnizam Abu Bakar, "Trust Model in MANET : An Overview".

[7] Abrar Omar Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", 2016 IEEE 30th International Conference on Advanced Information Networking and Applications.

[8] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, "GradeTrust: A Secure Trust Based Routing Protocol For MANETs" , 2015 International Telecommunication Networks and Applications Conference (ITNAC).

[9] Dr. Zeinab Movahedi, Zahra Hosseini, Fahimeh Bayan, Prof. Guy Pujolle, "Trust-distortion Resistant Trust Management Frameworks on Mobile Ad hoc Networks: A Survey", 2015 IEEE.

[10] Meenakshi Dubey1, P.S. Patheja2, Vijay Lokhande, "Reputation based Trust Allocation and Fault Node Identification with Data Recovery in MANET", IC4-2015.

[11] Muhammad Saleem Khan_, Daniele Midiy, Majid. I.Khan_, and Elisa Bertino, "Adaptive Trust Update Frequency in MANETs", 2015 IEEE 21st International Conference on Parallel and Distributed Systems.

[12] KefayatUllah! ,Rajib Das2,Prodipto Das!, Ananya Roy!, "Trusted and Secured Routing in MANET: An Improved Approach", 2015 International Symposiwn on Advanced Computing and Communication (ISACC).

[13] SJ. Indhu Lekha1 ,R. Kathiroli2, "SJ. Indhu Lekha1 ,R. Kathiroli2", 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[14] Heena1, Neeraj Kumar2, "Battery Power and Trust

Based Routing Strategy for MANET", 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[15] Hui Xia, Jia Yu1, Zhi-yong Zhang, Xiang-guo Cheng, Zhen-kuan Pan1, "Trust-enhanced multicast routing protocol based on node's behavior assessment for MANETs", 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications.

