An Attack Proof Trust Model for Secure Path Selection with Data Transmission in MANET: A Survey

Ravi Lodhi, Shiv Kumar, Babita Pathik

Abstract: A Mobile Ad-hoc Network (MANET) is a network of mobile nodes which also act as routers and are connected by wireless links. These routers are free to move and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. The dynamic nature of MANETs makes network open to attacks and unreliability. MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANETs is a legitimate challenge. Dynamic source routing set of rules is a functional protocol in wireless mobile ad-hoc network (MANET). Data Safekeeping and detection of malicious node in a MANET is an imperative job in any network. To achieve reliability and availability, routing protocols should be powerful against malicious attacks. This paper provides survey to the attacks while data transmission and finding secure route in MANET.

Keywords: MANET, secure routing, malicious attack, Ad hoc Network, Wireless Routing Protocol, trust value.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc. The issue of symmetric and asymmetric links is one among the several challenges encountered in a MANET. Another important issue is that different nodes often have different mobility patterns. Some nodes are highly mobile, while others are primarily stationary. It is difficult to predict a node's movement and pattern of movement. The dynamic nature of MANETs makes network open to attacks and unreliability. Routing is always the most significant part for any networks. Each node should not only work for itself, but should also be cooperative with other nodes. MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANETs is a genuine challenge.

Revised Version Manuscript Received on January 10, 2017

Ravi Lodhi, M.Tech. Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

Dr. Shiv Kumar, Professor & Head, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

Babita Pathik, Assistant Professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a noteworthy problem in the mobile Ad-hoc network. The distributed mobile nodes create links to form the MANET, which may include mischievous and selfish nodes. Developing the trust based system is very challenging problem in MANET. In order to filter out misbehaving nodes we propose a model which help in secure route discovery, data transmission and report to the MANET about any mischievous node. And also find secure data path for secure data transmission. We estimate the secure value of each node using timestamp of the operation. Then to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch network letdown.

II. BACKGROUND

The ideas dynamic source routing is created on the source transmitting which means the motivator of the data packet make available a systematic list of nodes rendering to which data packet pass through in the system. The key note this routing pattern is that intermediate nodes need not to track the information of the routing through which packet will traverse in the network as source node already has a decision regarding the routes. Utilization of source transmitting allows the data packet to travel in the loop free environment, elude the requirements for updating the routing information in the intermediate node, allows the node to forward the packet to store the moving info in them for future. All aspects of protocol operate entirely on demand [8]. DSR works in completely self-configuring and organizing without preexistence of structured network for slightly current system administration or substructure. The protocol works on the two important mechanisms. i.e. 'Route Discovery' and 'Route Maintenance'. Route discovery is a method of finding out the secure route in the network, when a source node's having a desire to transmit the data packet to the target node, where every node holds a route cache of source routes it has understood or overheard. Route maintenance [18] is the mechanism by which originator device recognize the alteration occurred in the network topology such that it understands about the longevity of the route available to the destination because of the node in the route list is moved out of the range.

DSR works on finding a route and uses that route called source route. Sender has a complete knowledge of particular sequence orders of the network nodes to reach at the destination. The initiator than pass this packet into the network interface wireless medium to the first node which is identified by the route in its route cache.

If that node is not the destined address, it forward the packet following by the further node mentioned in the route cache[9]. Once after another, process is continuous, until not reached to the final destination. After reaching to its desire end it will deliver the packet to the transport layer of the host.

III. LITERATURE REVIEW

Michiardi and Molva [19] propose CORE model, which only accepts positive recommendation by others. Consequently, this can lead to decreased efficiency of the system because nodes cannot exchange bad experiences from the misbehaving ones in the network. Also, CORE cannot be resilient against ballot-stuffing attack as it leaves ways for misbehaving nodes to collude and gain unfair high ratings. Wang et al. [20] propose a trust-based incentive model for self-policing mobile ad hoc networks to reduce the impact of false recommendation on the accuracy of trust value. However, the performance of the model is not tested against specific attacks such as bad-mouthing. Authors in [21] propose RFSTrust, a trust model based on fuzzy recommendation similarity, which is presented to quantify and evaluate the trustworthiness of nodes. They use similarity theory to evaluate the recommendation relationships between nodes. That is, the higher the degree of similarity between the evaluating node and the recommending node, the more consistent is the evaluation between the two nodes. In this model, only one type of situation is considered when selfish nodes attack is present and the performance of the model is not tested against other attacks related to recommendation. Soltanali et al. in [22], propose a model of trust to encourage the cooperation between nodes by using direct observation and recommendation. This model only accepts the last opinion of a node, which is passed to a reputation manager system at the end of each interval. Considering only the last opinion is not insightful enough to recognise the fluctuation in node's behaviour, like in on-off attack [12]. Li et al. in [10] include a confidence value in their evaluation by combining two values: trust and confidence into a single value called trustworthiness. They utilise the trustworthiness value to put weight on recommendations in which a recommending node with higher trustworthiness value is given more weight. Collusion attack in providing false recommendation is not considered by this work, and this may cause incorrect evaluation of the received recommendations [5]. Hermes [13] is a recommendation based trust model that uses an additional parameter known as an acceptability threshold (in relation to the confidence level). The notion of acceptability is used in the computation of recommendation to ensure that adequate observations of the behaviour of participating node has been obtained. However, the selection of acceptability is a trade-off between obtaining more accurate trustworthiness value and the convergence time required to obtain it. [10] provides information about routing security. It also provides detection of blackhole attack. It provides solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists, trust the intermediate node and send out the data packets. If not, just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network. A malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages, and begin to send data packets. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this may happen in a real situation. This paper does not provide group attacks problem. [11] provides information about recommendation based trust model for MANET. It successfully provides details and differentiated the honest and dishonest recommendations. Trust value algorithm Step 1 enumerates and lists the common neighbors between the evaluating node and the evaluated node. Step 2 selects the common neighbors listed in first part, having direct trust value greater than 0.5. The evaluating node sends request to the selected nodes to reply with recommendations about the evaluated node. Step 3 considers the recommendations received from neighbor nodes selected in second part and having a relationship as either friend or acquaintance. Using the recommendations considered indirect trust value of the evaluated node is calculated. This algorithm will not work on blackhole and location and time based attacks.

[12] provides Context-Aware Security and Trust framework (CAST) for MANETs, in which various contextual information, such as communication channel status, battery status, and weather condition, are collected and then used to determine whether the misbehavior is likely a result of malicious activity or not. Gossip-based Outlier Detection Algorithm For each node ni broadcast Vi to all of its immediate neighbors Upon reception of Vk from its immediate neighbor nk: merge Vi and Vk according to the rules calculate the top k outliers from TEMPi, and assign these k top outliers to Vi broadcast V ! i to all of its immediate neighbors. It will not detect selective and blackhole attacks which can provides many security problems. [13] provides Novel Key Management Technique in Three Tier (NKM_TT) Wireless Sensor Networks to manage the security methods in a WSN. It uses Message Authentication Code (MAC) to provide the data integrity. Digital signature grants authentication between the MS and AP as well as the Session Pairwise key provides authentication between AP and SN. Algorithm: E_TT and NKM_TT Step 1:Initially the MS wants to collect the data from particular SN. Hence, MS send data request to the AP. Step 2: The AP verifies the signature of the MS. Step 3: If the signature is valid then the AP send the join request message to the SN. Step 4: The SN checks the pairwise session key. Step 5: If the pairwise session key matches, then the SN sends the JRREP message to the AP. Step 6: Then the AP send RREP message to the MS. Step 7: The SN send encrypted data to the AP. MAC computation checks the integrity of data. Step 8: The AP collect the data from the SN and send this data to authenticated MS. This scheme decreases the PDR and response time of the network. [14] provides SIEVE, a fully distributed technique to identify malicious nodes.

SIEVE is very accurate and robustness under several attack scenarios and deceiving actions. SIEVE algorithm. SIEVE using LT code to prevent data from malicious node. It can mainly identify malicious node produces pollution attack. The techniques adopted for the identification and the following removal of malicious nodes clearly require a joint and careful design to optimize the overall performance. [15] provides survey of selfish nodes detection techniques in MANET. Algorithm Watchdog, misbehaving nodes are identified on the basis of packet dropped during the transmission of the next hop. When a node forwards packets, proper transmission of packets by the next node is verified by Watchdog. Misbehavior is noticed, If that node refuses to transmit the packets. The misbehaving nodes can be identified in the level of connection as well as in forwarding level, The problem of all techniques are manual allocation of trust value not automatically. It also have limitation which will not provide more effective infrastructure-free authentication in ad hoc networks assuming that identities need not be entirely stable at the routing level, but that spoofing of other nodes is unacceptable. To design a robust trust management framework. A hybrid trust management framework (HTMF) to construct trust environment for MANETs. Hybrid trust management algorithm if (it has not been received before) {receive this information and perform deviation test and one check; if (bad mouthing attack is detected) { drop this information; update the trustworthiness of information provider in recommendation generation system. }else{ obtain the trustworthiness of the provider from recommendation generation system; update ITF; distribute such message to its neighbors. } }else{ drop the message. }The limitations is it will not work on selective misbehave attack and location and time attacks. [17] provides survey of various threads and malicious attacks in MANET Cooperative Bait Detection Algorithm. The CBDS approach combines both the proactive and reactive mechanisms. In this scheme the address of the nearby node is used as the bait destination address to detect the address of the compromised node using reverse routing technique. The address of the detected node is added to the black hole list. The other nodes are also informed about the black hole node. The destination can also trigger this scheme it there is decrease in packet delivery ratio. Steps are Initial bait, initial reverse tracing, shifted to reactive defence step. [18] paper only provides survey to the blackhole, grayhole, and rushing attacks. The location based and time based attacks are not surveyed in this paper. It provides recommendation based trust model with a defence scheme, which utilises clustering technique to dynamically filter out attacks related to dishonest recommendations between certain time based on number of interactions, compatibility of information and closeness between the nodes. It only detect bad mounting attack. It does not provide location and time based attacks.

IV. CONCLUSION

Ad-hoc network doesn't depend on any central administration or stable infrastructure such as base. Determination of link failure, data security, detection of malicious node and secure information transmission in a MANET is an important task. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. DSR set of rules is a sensible protocol in wireless mobile ad-hoc network. The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a remarkable difficulty in the mobile Ad-hoc network. Due to the intrinsically self-motivated nature of the mobile network topology, the existing routes cannot be secure. Ad-hoc network using dynamic source routing under malicious attack with secure routing and data transmission. The paper provided trust based model for MANET for Secure Path Selection with Data Transmission in MANET.

REFERENCES

1. Tanvi Arora, Amarpreet Kour, Mandeep Singh," Review of various routing protocols and routing Models for MANRTs", International Journal of Innovation & Advancement in CS ,IJIACS,ISSN 2347-8616,Vol.4 Special Issue, MAY 2015.
2. Amit N Thakre ,Mrs M.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network", MANETs 2010
3. David A. Maltz, "On demand routing in multi-hop wireless mobile ad-hoc network" CMU-CS-01-130, PhD. Desertion, School of computer science Carnegie Mellon University, Pittsburgh PA- 2001.
4. Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2115
5. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct. 2002.
6. B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security. New York, NY, USA: Springer, 2007, pp. 103–135.
7. N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop ad hoc networks," in Proc. Netw. Netw. Technol., Services, Protocols; Perform. Comput. Commun. Netw.; Mobile Wireless Commun., 2004, pp. 1446–1451.
8. S. Buchegger and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.
9. G. V. Crosby, L. Hesterand, and N. Pissinou, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," Int. J. Netw. Security, vol. 12, no. 2, pp. 107–117, 2011.
10. Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE 2002, pp-70-76
11. U. Venkanna, R. Leela Velusamy, Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks, ERCICA 2013, pp-123-130
12. Wenjia Li, Anupam Joshi, Tim Finin, CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies, Distributed and Parallel Database 2013, pp1-26
13. Senthil Kumar and E. Logashanmugam, Novel Key Management Techniques in Three-Tier Wireless Sensor Networks, IJCTA 2016, pp-903-910
14. R. Gayathri, J.Maria Sofi Anusuya, Preventing Malicious Node and Provide Secure Routing In Manet, IOSRJECE 2015, pp.9-13
15. Aniket Patil,Javed Khan,Ashish Khandave,Abhishek Yadgire, Monika Dangore, Selfish Nodes Detection Techniques in MANET-A Survey, IJRASET 2015, pp.286-291
16. Ruidong Li, Jie Li, Peng Liu, Jien Kato, A Novel Hybrid Trust Management Framework for MANETs, IEEE 2009, pp.251-256
17. P Suganya, CH Pradeep Reddy, Potential threats caused by malicious nodes and various counter measures available in MANET: A Survey, RJPBCS, June 2016, pp-1012-1017
18. Antesar M. Shabut, Keshav P. Dahal, Senior Member, IEEE, Sanat Kumar Bista, and Irfan U. Awan , Recommendation Based Trust Model with an Effective Defence Scheme for MANETs IEEE Oct. 2015, pp.2101-211

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.