International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

SDSR-A New Hybrid Secure Routing Protocol using Trust Recommendations in MANET

Sesha Bhargavi Velagaleti, M.Seetha, S.Viswanadha Raju

Abstract: ***A mobile ad hoc network is a dynamic network which can be established when there is no possibility or if it is practically impossible to establish a standard cellular infrastructure for communication. It is a form of decentralized wireless network where nodes are independent of each other and operate on their own. Every node is free to move in and out of the network as and when needed. This also introduces many concerns about security of data being forwarded through these nodes as there is no fixed dedicated mechanism to verify the authenticity of the nodes that join and leave the network at varied times. As MANET is a multi-hop network, data should be forwarded through many intermediate nodes, before it actually arrives at the intended destination. So data on transit through these intermediate nodes should be protected from any malicious nodes. Different protocols were proposed in literature that address the security concerns of routing considering varying parameters. This paper illustrates a hybrid routing protocol, SDSR Secure Dynamic Source Routing Protocol which takes the recommendations of neighbour nodes to judge about node's authenticity and uses that information to calculate the trust value of a node. Using trust values of nodes, malicious nodes are identified and those nodes are excluded from data transmission path between the source and destination. The performance of SDSR is also evaluated in terms of efficiency parameters like Packet Delivery Ratio, Packet Loss, Communication Overhead, Throughput etc., and results are presented. This protocol can also be compared with existing routing protocols proposed for MANETS in terms of various quality of service parameters.***

Keywords: The performance of SDSR

I. INTRODUCTION

Network Security is an emerging area now a days, in particular the area of mobile ad hoc networks is seeing a visibly vast growing technology. Lot of research is being contributed in the area of ad hoc networks to improve efficiency in terms of various quality of service parameters like packet delivery ratio, communication overhead, packet loss etc., There has been a wide range of study with regard to routing security where data is transmitted between source to destination, there is a need for protecting the integrity and confidentiality of the data by allowing only authenticated notes to participate in communication. But the characteristics like dynamic topology, infrastructure less operation, varying bandwidth requirements, energy constraint nodes, limited physical security and multi hop communication of MANET makes the task more challenging.

Revised Manuscript Received on June 15, 2020.
* Correspondence Author
Sesha Bhargavi Velagaleti*, Assistant Professor, IT Departmnet, GNITS, Shaikpet, Hyderabad, India.
Dr.M.Seetha, Professor, CSE Departmnet, GNITS, Shaikpet, Hyderabad,India
Dr.S.Viswanadha Raju, Professor, CSE Departmnet, JNTUK, Hyderabad, India.

In spite of these challenges, MANETS found their way in many emerging application areas like educational and medical fields, military and defence operations, emergency and rescue operations like earthquakes and natural calamities, disaster relief management etc., The multi hop communication of MANETs makes routing a challenging task. There were several routing protocols described in literature. These routing protocols are classified as either static or dynamic based on the time at which the decision on next node is taken during routing process. They can also be characterized based on the way their routing tables are updated and used in routing data packets. The other class of protocols which take the advantages of both these static and dynamic protocols are called as hybrid routing protocols. They either take location based information or geographical information of nodes to maintain their routing tables. This paper implements a hybrid routing protocol that takes the recommendations of neighbour nodes to evaluate the trust value of the nodes which can be used to identify the malicious nodes that are responsible for packet drops, packet loss during data transmission.

II. RELATED WORK

There were many routing protocols proposed in literature to deal with the issues in routing protocol. In a paper[1] titled " Secure Neighbor Discovery System for ad-hoc through AASR Protocol ", a new protocol called TQoS (Trust Based Quality of Service) which uses key encryption onion based routing but there is no elimination of malicious nodes during data transmission. So data cannot be protected from malicious nodes during transmission to destination. In another protocol called SEAD: (Secure and Efficient Ad hoc Distance vector routing protocol) [2] , authors proposed a new methodology to prevent DoS attacks in a network, but they did not address the problems with multiple malicious nodes. In , " Trusted and Secured Routing in MANET: An Improved Approach "[3], authors proposed a trust based security model using trust quantification which assumes nodes already are authenticated and genuine. This algorithm also works for only single malicious nodes, but does not provide a solution when multiple nodes cooperate with each other and try to launch an attack. In TAODV (Opinion Based Trusted Routing Protocol) [4], opinion of the nodes is considered for routing data between the nodes. Nodes change their opinions based on the opinions received from the other nodes. This algorithm fails to address the issues caused due to internal attacks.

An extended DSR routing is proposed in TR-DSR (A routing Protocol Based on Trust) [5], in which trust information is the basis for routing, but this algorithm has huge communication overhead and multiple malicious node detection is also not effective. An extension to AODV algorithm is suggested in AOTDV (Trust-based on-demand multipath routing in mobile ad hoc networks) [6] in which misbehaving nodes may not give proper reliable information in calculating the path trust in case of any colluding attacks. In Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks [7] , source based secure routing protocol was proposed based on AODV routing , but it adds more delays in data transmission and cannot identify the issues with multiple malicious nodes. In a paper titled "Energy Aware Trust Based Routing Scheme for Mobile Ad-hoc Networks"[8], methods to reduce transmission overhead and power consumption in MANETs were discussed which help save batter life of the nodes. Energy consumption of the nodes during data transmission from a source to destination was addressed in this paper. In [9] "TBSRP: Trust Based Secure Routing Protocol for WSNs", a reliable communication approach using trust vectors to take a decision on net hop a node should make is proposed. Results are analysed in terms of metrics like delivery ratio by comparison with AODV protocol.

1. SDSR (Secure Dynamic Source Routing) Protocol

This protocol finds a secure path for data transmission between a given source and destination nodes using the trust values of the nodes, thus by identifying and eliminating the malicious nodes in the path for data transmission. When the source node has data to transmit, it forwards the request RREQ packet to all the neighbouring nodes with the goal of finding a secure path to the intended destination node. All the adjacent nodes upon receiving the request packet, verify their routing tables for route to destination, and if path exists, composes a RREP packet containing route to destination and forwards it to source node. If a route to destination node does not exist, the request packet is forwarded to their neighbouring nodes by appending their identity. This process is repeated until a route to destination is found by the source node. Upon reception of route information about the destination node, the source node can computes the final trust value of the nodes based on the primary and secondary trust values received by the neighbouring nodes. Using this trust value calculated, source node can identifies whether a node is malicious or trusted one. The trust value of the nodes acts as a measure here to compute the trustworthiness of a node based on which a decision to include a node into a route to destination is taken by the source node. If a node is identified as malicious node, that information is broadcasted to all the neighbouring nodes. Following figure fig3.1 illustrates the overall framework of the SDSR protocol.

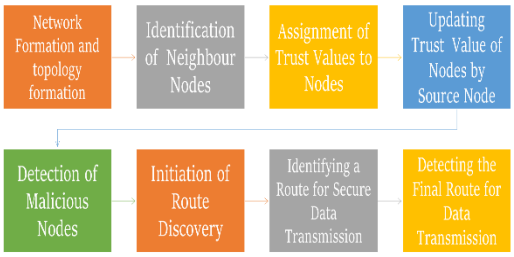

Fig 3.1. SDSR Protocol Framework

Initially Primary Trust, Temporary Trust, Functional Trust, Recommendation Trust and Final trust are all set to zero. Source node keeps a count of the number of control and data packets it has forwarded to its neighbours, successfully forwarded and dropped packets. Using this value, the source node computes the Primary Trust value of all the nodes. From the obtained Primary Trust, a node's functional Trust is also evaluated by the source node. To find the trust information of nodes which are not neighbours, the source node requests for recommendations from its neighbour nodes about their neighbour nodes. Source collects the Recommendation trust of all non-neighbour nodes in the network. Both Functional Trust and Recommendation trust together are used to evaluate the Final trust value of a node.

2. Performance Analysis of SDSR Protocol

Various performance metrics like Packet Delivery Ratio, Packet Loss, and Communication overhead, Throughput etc., are evaluated under different simulation scenarios. Number of nodes is set to 50.

4.1 Performance Analysis on PDF:

With the detection of malicious nodes and hence making a path with secure nodes to the destination, there is an increase in the PDF ratio in SDSR protocol when compared to existing protocols proposed for MANETs. Using the trust based information about the nodes on the path to destination makes it easy to identify the malicious and hence helps in finding alternates path dynamically which results in improved PDF across the network.

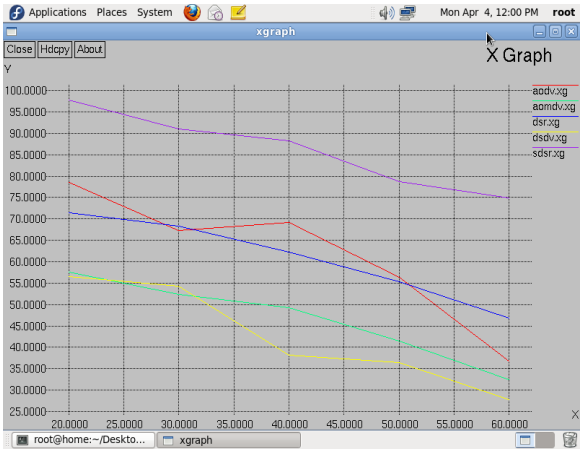

Fig. 4.1 Xgraph showing PDF Vs. Pause Times

4.2 Performance analysis on Throughput:

This performance of this algorithm w.r.t. throughput is an improvement over the existing ones, which shows that at different stop times the throughput gradually increases which shows that more number of data packets can be transmitted on the identified path within a prescribed unit of time.

4.3 Performance analysis on End to End Delay:

While transmitting the packets from source to destination, as the nodes are wireless and therefore use a wireless physical channel, due to its properties like reflection and refraction, link failures, delays occur in transmission of packets from source to destination.

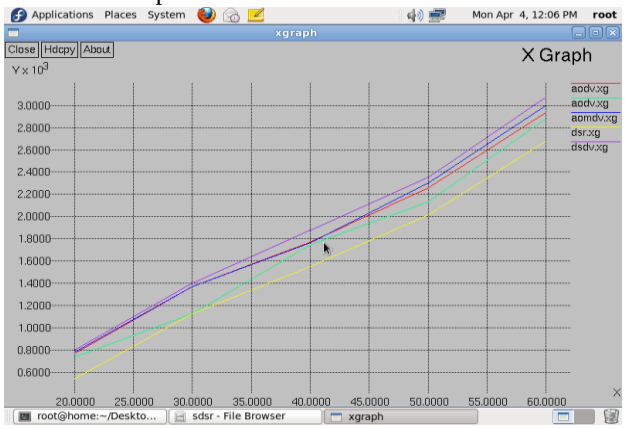

Fig. 4.2 Xgraph showing Throughput (Received Packet Size Vs. Start and Stop Times)

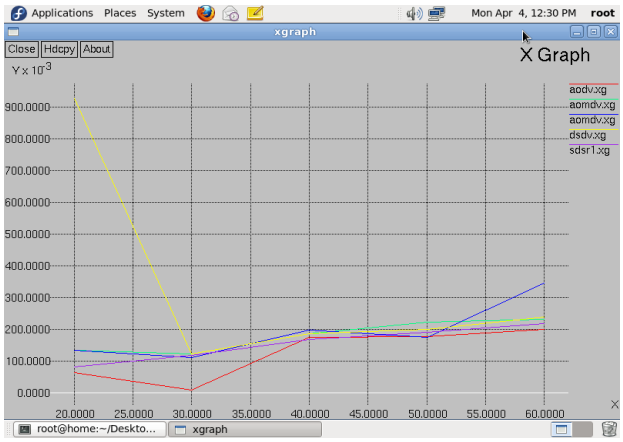

Fig. 4.3 Xgraph showing End to End Delay Vs. Start & Stop Times

Few packets are discarded if the packets are lost after the threshold time limit. The table in previous slide illustrates the delay in msec caused at various pause times. As the number of packets and their size increase, end to end delay also gradually increases. This is reduced in this protocol by selecting a reliable shortest path from source to destination. Even though the number of malicious nodes increase, there is not significant decrease in the performance metrics as trust evaluation is still done more co-operatively, SDSR succeeds in detection of presence of malicious nodes, so the performance of the protocol is not affected. There is a slight increase in the overhead as little more number of control packets are generated to exchange information about these malicious nodes.

4.4 Performance analysis on Packet Loss:

Due to the transmission errors and the harmful and mischievous operation of malicious nodes, few packets are lost on their way from source to destination. This results in a reduced PDF across the network which is not desirable. So in this SDSR protocol, the packet loss is drastically reduced by identifying the malicious nodes using trust metrics and verifying the nodes authenticity and hence it was seen that the secure path from source to destination is a path that excludes these nodes on the path.

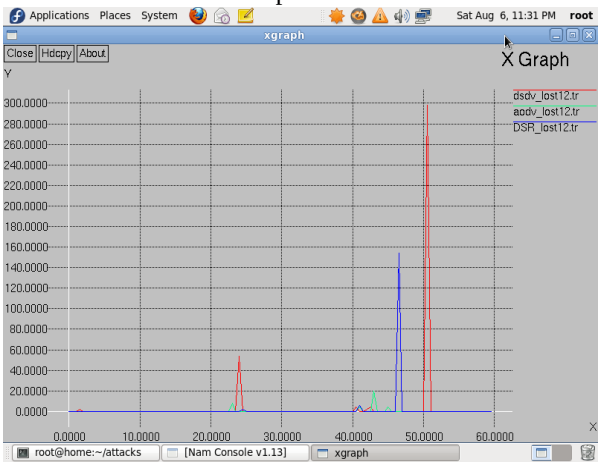

Fig. 4.4 Xgraph showing Packet Loss Vs. Start & Stop Times

4.5 Impact of varied number of malicious nodes on the performance of SDSR

Figure 4.5 illustrates the scenario of change in the number of malicious nodes in the network on various performance metrics when the number of nodes is set to 50. Even though the number of malicious nodes increase, there is not significant decrease in the performance metrics as trust evaluation is still done more co-operatively, SDSR succeeds in detection of presence of malicious nodes, so the performance of the protocol is not affected. There is a slight increase in the overhead as little more number of control packets are generated to exchange information about these malicious nodes.

S. No.	No. of Malicious nodes	PDF	End-to-End Delay	Throughput	Overhead	Packet Loss
1	1	94.56	0.10962	16304.02	1658	18
2	2	97.6391	0.2317	1625.21	2453	36
3	4	96.587	0.4581	164..237	2617	51
4	8	96.12	0.4752	1612.095	2939	93

Fig. 4.5 Table showing impact of varied no. of malicious nodes

III. CONCLUSION AND KEY FINDINGS

An implementation of routing protocols proposed for MANET was done and found that various existing routing protocols doesn't address the security issues in MANETs. Various proactive and reactive protocols like AODV, DSR, and DSDV were implemented using diverse parameters. Performance Analysis of these existing protocols was done by considering metrics like Packet Delivery Fraction, Throughput, Packet loss, End to End delay, Overhead etc. to emphasize their behavior in different scenarios. Most of them exhibited better performance when there is no mischievous behavior but the number of packet drops gradually increased in the presence of malicious nodes.

A new hybrid secure protocol SDSR which can work for both proactive and reactive protocols has been proposed and implemented which reduced packet loss, end to end delay and improved packet delivery ratio, throughput even in the presence of malicious nodes. This protocol reduced the possibility of occurrence of attacks using metrics like Primary trust, functional Trust and recommendation trust to identify a secure trusted path between source and destination. Because of the use of trust information about the nodes, the authenticity of the nodes was easily verified and hence the time required for source to choose an alternate path is downsized. By varying the simulation scenarios with different types of attacks and variable packet sizes, optimal performance of the protocol can be accomplished. SDSR can be improved to find the best route to destination in much more shortest time possible that reduces the overall delay. Implementation with varied QoS parameters can be visulaised.

REFERENCES

1. S.Arun Karthick k.Sudhakar , " Secure Neighbor Discovery System for ad-hoc through AASR Protocol ", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.6, December 2014 .
2. K. Thamizhmaran, R. Santosh Kumar Mahto, V. Sanjesh Kumar Tripathi, " Performance Analysis of Secure Routing Protocols in MANET " , International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012,, ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.
3. Kefayat Ullah, Rajib Das, Prodipto Das, Ananya Roy , " Trusted and Secured Routing in MANET: An Improved Approach ".
4. X. Li, M. R. Lyu, and J. Liu, " A Trust Model Based Routing Protocol for Secure Ad Hoc Networks ", Proc. Aerospace Conference, IEEE, vol. 2, pp. 1286-1295, 2004.
5. C. Wang, X. Yang, and Y. Gao, "A Routing Protocol Based on Trust for MANETs ", Springer-Verla, 2005, pp. 959–964.
6. X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, " Trust-based on-demand multipath routing in mobile ad hoc networks ", Information Security, IET, vol. 4, issue 4, pp. 212-232, Dec 2010.
7. A.Menaka Pushpa, " Trust Based Secure Routing in AODV Routing Protocol ",Internet Multimedia Services Architecture and Applications (IMSAA), IEEE conference, pp.1-6 , 2009.
8. Suyash Bhardwaj, Isha Bhardwaj, Poornima Tyagi "Energy Aware Trust Based Routing Scheme for Mobile Ad-hoc Networks", Journal of Basic and Applied Engineering Research Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 9; October, 2014 pp. 105-109.
9. Anuradha and Amita Malik "TBSRP: Trust Based Secure Routing Protocol for WSNs", Proceedings of the International Conference on" Emerging Research in Computing, Information, Communication and Applications", ERCICA 2013, ISBN:978931071020.
10. Lohit Kumar, Vishali Sharma, ―An Overview of MANETs: Issues and Security Solutions, IJETT journal, Volume-10, Number 11, Year of Publication 2014, DOI:10.14445/22315381/IJETT-V10P301
11. C Sreedhar , Varun Varma Sangaraju ,A Survey On Security Issues In Routing In MANETS IJCOT Journal Volume-3 Issue-9 Year of Publication Oct 2013
12. V. Sesha Bhargavi, M. Seetha, S.Viswanadharaju. "A trust based secure routing scheme for MANETS", 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 2016
13. **J.** Mc.Quillan et al. "The new Routing Algorithm for the ARPANET", IEEE Transactions, May 1980.
14. J.J. Garcia-Luna-Aceves. "A Unified Approach to Loop free Routing using Distance Vector and link states or Distance Vectors.",ACM SIGCOMM Computer Communications Review, Vol.19, No. 4, pp.212-223:September 1989.
15. V. Sesha Bhargavi, S. Viswanadha Raju. "Enhancing security in MANETS through trust aware routing", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016
16. Charles E. Perkins, Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", SIGCOMM 94 -8/94 London England UK, 1994 ACM 0-89791 -682-4/94/0008
17. Johnson David A. Maltz, in "Dynamic Source Routing in Ad Hoc Wireless Networks", book chapter in Mobile Computing, T. Imielinski, and H.Korth, 1996.
18. V. S. Bhargavi, M. Seetha and S. Viswanadharaju, "A hybrid secure routing scheme for MANETS," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, 2016, pp. 1-5.