# Secure Route Discovery using Opinion Based Method in MANET

Dr.S.Revathi,
Associate Professor, Dept. of CSE
B.S.Abdur Rahman Univeristy,
Chennai, India
srevathi@bsauniv.ac.in

Dr.T.R.Rangaswamy,
Dean(Academic Affairs),
B.S.Abdur Rahman University,
Chennai, India

***Abstract— A Mobile Ad-Hoc Network (MANET), each node can move around freely, as the network topology changes dynamically. Malicious nodes may disrupt routing algorithms by transmitting a false hop count by dropping data packets, and by routing the packets through unintended routes, and so on. Hence a secure route discovery is required. In the proposed model called Secure Route Discovery using Opinion Based model (SRDO), each node in a MANET predicts its neighbor's future behaviours and selects the shortest faithful route during route discovery phase to transmit the required packets. The objective is to design a security system and to keep the overhead as low as possible, during route discovery and optimizing the output.***

***Keywords-Secure Route, opinion based model, SRDO***

## I. INTRODUCTION

If all the nodes in the network behave co-operatively, then the network works well. Due to openness in network topology and absence of a centralized administration in MANET, it is vulnerable to various attacks from malicious nodes. To enhance the security of network and to avoid the hazards from malicious nodes, an opinion based model is proposed based on the historical behaviors and predict the future opinion of the node. This opinion based model is implemented by calculating the opinion of the nodes. The proposed protocol, Secure Route Discovery using Opinion Based Method (SRDO), is used to discover a secure route during route discovery phase.

## II. RELATED WORK

Zouridaki et al (2009) proposed E-Hermes which is a robust cooperative trust establishment scheme for mobile ad hoc networks. In this each node determines the trustworthiness of the other nodes with respect to reliable packet forwarding by combining first-hand trust information obtained independent of the other nodes, and second-hand trust information obtained via recommendations from other nodes.

Poonam et al (2010) provided a survey of the work done in the field of trust based security in MANET routing protocols. Poonam et al (2011) Imran & Hussain (2008) discussed malicious node identification by the behavior of the neighbor nodes. The neighbor node behavior is calculated by the opinion or through the guard node, and the misbehaving node is identified. After deciding which node misbehaves, they eliminated it from the network topology.
Nan et al (2010) proposed a new IDS called Enhanced Adaptive Acknowledgement (EAACK) that solves four significant problems of the Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehaviour report. Praveen (2010) described the different types of network layer attacks and the countermeasures for each type of attacks.

All the above schemes only try to protect the system from the attacker, but do not bother about quarantining the attackers. The twin systems of watchdog and path rater (Sergio et al 2000), not only detect the mischievous nodes but also prevent their further participation in the network. Hao et al (2006) stated that SCAN also has a similar action, but is more comprehensive, in the sense that not only packet dropping but also other misbehaviours like giving the wrong hop count are covered.

`Sanjay et al (2011) proposed Friend based Ad hoc routing using the Challenges to Establish Security algorithm to provide secure routing in Mobile Ad hoc Networks. They have Sharing Friend Lists consisting of the list of trusted nodes to the source node only through which the data transmission takes place finally. The friend list's node is rated based on the amount of data transmission and its friendship with other nodes in the network.

Zhi et al (2011) proposed a trust management scheme consisting of two auto regression models, called Autoregressive (AR) model and Autoregressive with exogenous inputs (ARX) model to improve the routing reliability for wireless ad hoc networks. In the AR model, the node uses its own observations for prediction, while the ARX model uses information from the other neighbors.
Soufiene et al (2011) presented a comprehensive survey on the investigations of the state-of-the-art countermeasures to deal with the packet dropping attack**.** They compared the different schemes such as the Passive Feedback based, ACK-based, Reputation-based and Incentive-based schemes with their assumptions and limitations.

Hui et al (2013) proposed trust prediction and trust-based source routing in mobile ad hoc networks. They presented a dynamic trust prediction model to evaluate the trustworthiness of nodes. This is based on the nodes' historical behavior, as well as the future behavior via extended fuzzy logic rules prediction. They have integrated the trust predication model into the Source Routing Mechanism. They chose the shortest route that meets the security requirement of data packet transmission.

Janvon et al (2012) focused on networks using the popular AODV protocol and a secure extension of the AODV, the Secure AODV (SAODV) protocol. They conducted a vulnerability analysis of SAODV to identify unresolved threats to the algorithm, such as medium access control layer misbehavior and Wormhole attacks, Rushing attacks, Blackhole attacks, Resource depletion attacks, Distributed Denial of Service (DDoS) attacks and Jellyfish attacks.

Govindan & Mohapatra (2012) presented a detailed analysis of trust dynamics including trust propagation, prediction and aggregation algorithms in MANETs. They have also classified the trust computations into two types: i) Distributed trust computations: Every node computes its own value of trust of its neighbors and ii) Centralized trust computations: a Central agent manages/helps the node in trust computations. They again classify the Distributed trust computations as: Neighbor sensing (Direct trust), Recommendations based trust (Indirect trust), and Hybrid method. The trust agent based method is an example of centralized trust computation.

Venkataraman et al (2013) proposed a regression based trust model for Mobile Ad Hoc Networks. They proposed a generalized Vector Auto Regression (VAR) based trust-model over routing protocols that can monitor every functional behaviour of a neighbouring node. This model identified multiple attacks simultaneously in wireless ad hoc networks and worked well for proactive and reactive routing protocols. This is done by strengthening the evidence collection phase prior to trust evaluation. In this approach, the trust can be easily incorporated, independent of the underlying network layer routing protocol, in wireless networks.

.

## III. PROPOSED ALGORITHM

### *A. Secure Route Discovery*

In the proposed protocol, by using Opinion Based Method, each node calculates the behavior of its direct neighbor nodes, and this opinion value is stored in the routing table. To find the route from source to destination, the source node broadcast the RREQ packet to its neighbors. If the RREQ packet reaches the destination, the opinion value which was stored in routing table is checked, whether the intermediate node is a malicious or not. If the intermediate node is not a malicious node, the RREP packet adds the opinion value in the RREP and forwards it to the next node in the reverse route to the source node. Otherwise -1 is set in the opinion field and the intermediate node will never update it. Whenever the RREP reaches the source node, the source node checks the RREP field. If the RREP packet value is -1 then it is identified that there is at least one malicious node in the route. The proposed protocol SRDO not only reduces the average end-to-end delay, but also constructs the secure route.

### B. *Opinion Based Method*

The Opinion Based Method will continuously track the behavior of its neighbors and compute their opinion of every node. The proposed method capturing the behavior of the neighbor node(ie data forwarding ) and opinion value of the neighbor, is expressed as the number of data packets received from the neighbor to the total number of data packets forwarded to the neighbor. This model relies on the direct observations of neighboring node.

The computed opinion value is stored in the routing table. The computed opinion value reflects the neighboring nodes' behavior and identifies the malicious node based on the opinion value.

### C. *Propagation of opinion values*

During route discovery phase, every node in the network computes the opinion value by using the Opinion Based Method, which exchange these values among the neighbour nodes. The original RREP packet is modified as shown in Figure 1.1 and it is implemented over the AODV, to include the opinion value in the modified RREP as shown in Figure 1.2. The source node initiates the route discovery process by sending the RREQ packet. Whenever the destination node recevies the first RREQ, the destination node will send a RREP message without any opinion information in the message, while, the intermediate node receiving the RREP, adds the opinion value of the destination node in RREP, and forwards it to the next node in the reverse route to the source. As the RREP packet proceeds towards the source, the intermediate nodes add the opinion values of the neighbor nodes, only if they are not malicious. If it is a malicious node, the opinion value of -1 is set in the opinion field. If the intermediate nodes receive negative values in the opinion field, they will never update the opinion value. Hence, the source node can identifies that there is at least one malicious node in the route to destination, and the route will not be selected for the transmission of data.

| Type | R | A | Reserved | Prefix Sz | Hop Count |
|---|---|---|---|---|---|
| Destination IP Address | | | | | |
| Destination Sequence Number | | | | | |
| Originator IP Address | | | | | |
| Lifetime | | | | | |

***Figure 1.1 Original RREP packet format in the AODV***

| Type | R | A | Reserved | Prefix Sz | Hop Count |
|---|---|---|---|---|---|
| Destination IP Address | | | | | |
| Destination Sequence Number | | | | | |
| Originator IP Address | | | | | |
| Lifetime | | | | | |
| Opinion Value | | | | | |

***Figure 1.2 Modified RREP message format in the SRDO***

#### IV SIMULATION RESULTS

The SRDO calculates a node's opinion using the Opinion Based Method, based on the previous history, and provides a relative identification of the malicious node. To evaluate the performance of the proposed protocol SRDO, we have conducted a comprehensive test, using the NS2- network simulator.

### *Experimental Setup*

The NS2 simulator is used to evaluate the performance of the SRDO in different conditions. Consider a network topology of 1000 × 1000 m, in which n nodes are randomly placed. Each node has a uniform default transmission range of 250 m. With a fixed transmission range and network area, the network density is varied from low to high, by altering the number of nodes. Each simulation is run for 600s, and repeated 8 to10 times. The parameters used in the simulations are listed in Table 1.1.

**Table 1.1 Simulation Parameters**

| Parameters | Values |
|---|---|
| Transmission range | 250 m |
| Number of nodes | 50-120 |
| Number of comm. pairs | 10 |
| Network area | 1000 $m^2$ |
| Mobility model | Random way point |
| Mobile speed | 0-25 m/s |
| Routing policy | AODV |
| Traffic type | CBR (constant bit rate) |
| Packet sending rate | 5 packets/s |
| Antenna | Omni antenna |
| Path loss model | Two-ray ground |
| MAC protocol | 802.11 DCF |
| Interface queue type | DropTail/PriQueue |
| Simulation time | 600 s |
| Pause time | 100 s |

### *Performance Metrics*

The important metrics on which the DRSR and the proposed protocol SRDO are evaluated, are the data delivery rate, control overhead, and average end-to-end delay.

**Network Throughput**- Throughput indicates the amount of digital data transmitted per unit time from the source to the destination.

**Routing Packet overhead**- The total number of control packets sent out by all the nodes divided by the total number of successfully delivered data packets.

**Average end-to-end delay**- The average time taken by the data packet from the source to the destination, including buffer delays during route discovery, queuing delay at interface queue, retransmission delay and propagation time.

**Varying Node Speed:** The objective of the simulation setting is to evaluate how the protocols, namely, the DRSR and the SRDO perform, on varying the node speed from 0(m/s) to 30 (m/s).

### *Network throughput*

Figure 1.3 (a) shows how the protocols the DRSR (Revathi et al) and the SRDO perform at the maximum speed of nodes varying from 0(m/s) to 30 (m/s). The throughput of DRSR decreases remarkably as the nodes speed up, while that of the SRDO decreases gently. At high speed, the differences become noticeable. The reason is that the SRDO uses the opinion feature to detect the node behavior which increases the probability of successful delivery to a good opinion node using a trusted route. The DRSR maintains the shorter route to the destination, and it is unable to improve the throughput in the case of attacks from malicious nodes. The throughput of the DRSR is 0.2 packets/sec, and that of the SRDO is 0.35 at the simulation speed of 10 (m/s). The proposed protocol improves the throughput by 65% at the simulation speed of 10 (m/s). When the speed is increased to 30 (m/s), the proposed protocol improves the throughput by 80%.

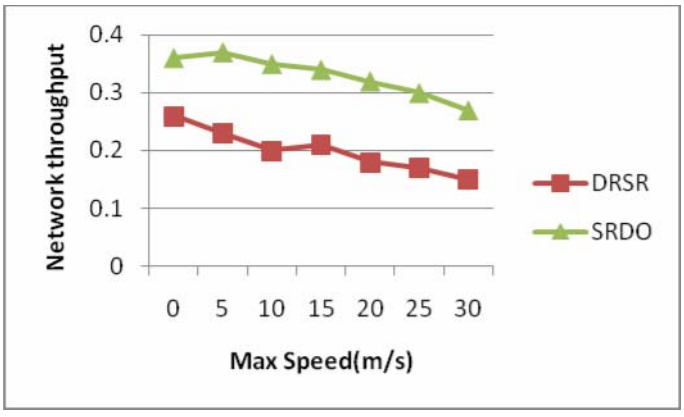

**Figure 1.3 (a): Network Throughput varying the node speed**

***Routing packet overhead***

From Figure 1.3 (b), the routing packet overhead in the DRSR and SRDO rises with the increase in the maximum speed, due to which the route link breaks down easily. Whenever the speed increases, the routing packet overhead in the SRDO remains comparatively higher than that in the DRSR. The reason is that i) more control packets need to be sent on qualified routes to meet the opinion requirement of the SRDO. But, in the DRSR, the security is not incorporated. ii) The additional route updates packet increases the number of control and routing packets in the SRDO. From the figure, it is identified that the routing packet overhead in the SRDO is increased 8.3% , 4.16% and 3.45% at the speed of 0(m/s), 15 (m/s) and 30 (m/s) respectively compared to DRSR. Even if the routing packet overhead is increased, the proposed protocol SRDO achieves greater enhancement of network security.

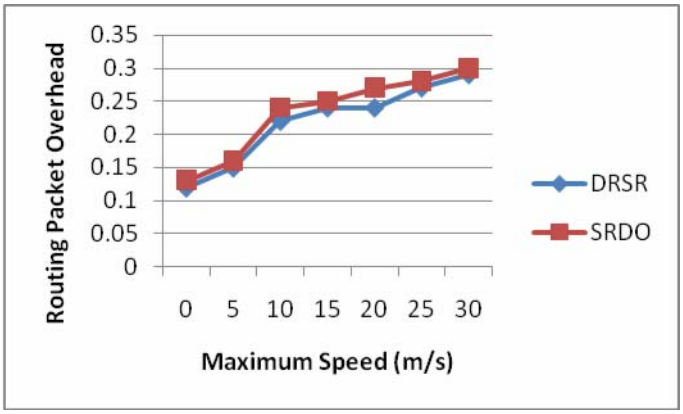


**Figure 1.3 (b): Routing Packet overhead varying the node speed**

***Average end-to-end delay***

Figure 1.3 (c) shows that the average end-to-end delay increases with an increase in the max speed. The SRDO has less average end-to-end delay than the DRSR. The reason is that the SRDO avoids malicious nodes more accurately, thus reducing the risk of added delay for presenting the failed routing packets. At higher speeds, the route entries become invalid more quickly, and thus the source node initiates route rediscoveries before sending the data. The average delay is reduced 8.3%, 4.16% and 3.44% compared to DRSR at the speed of 10 (m/s), 15 (m/s) and 30 (m/s) respectively.

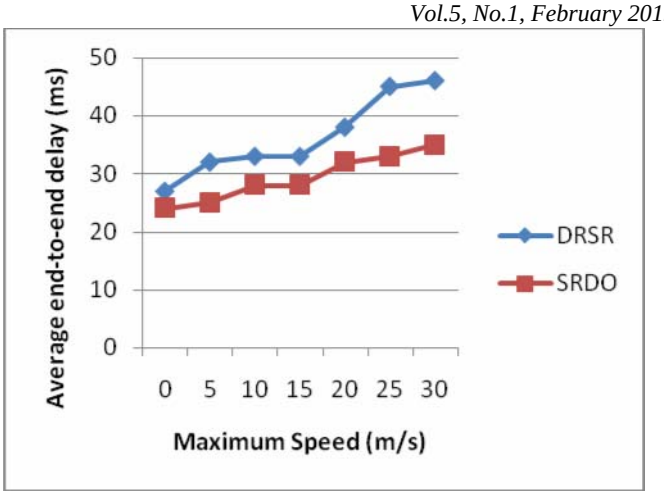


**Figure 1.3 (c) Average end-to-end delay varying the node speed**

## V CONCLUSION

The proposed protocol SRDO constructs the secure route uses the opinion based method during the route discovery phase. In the proposed protocol called SRDO, each node in a MANET predicts its neighbor's future behaviours, by using the Opinion Based Method, and selects the shortest faithful route during the route discovery phase to transmit the required packets. The opinion based scheme does not consume network resources in terms of computational complexity, memory and message overheads, as it were implemented using the neighbor's opinion. The proposed protocol SRDO significantly improves the performance, compared to the Dynamic Route Shortening and Repairing Mechanism (DRSR). It adapts itself well in a very dynamic network environment. The performance of the SRDO has been studied, using simulations under varying the speed and the number of malicious nodes. All these simulations demonstrate that the SRDO outperforms than the DRSR, in terms of packet delivery ratio and end-to-end delay, while it reduces the routing overhead significantly.

## REFERENCES

[1] Zouridaki, C, Mark, B, Hejmo, M & Thomas, R, 'E-Hermes: A robust cooperative trust establishment scheme for Mobile Ad hoc Networks", Journal of ELSEVIER Ad Hoc Networks, vol.7, no. 6, pp. 1156-1168,2009

[2] Poonam, Garg, K & Misra, M , "Trust Based Security in MANET Routing Protocols: A Survey", A2WiC "10, September 16–17, pp.47-53,2010

[3] Poonam, Garg, K & Misra, M 2011, "Eliminating misbehaving nodes by opinion based Trust Evaluation Model in MANETs, ICCCS"11, ACM, pp.50-55.

[4] Imran, R & Hussain, SA , "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", Elsevier Computer Communication, vol. 3, pp.1796-1802,2008.

[5] Nan, K, Elhadi, MS & Tarek, RS, "Detecting Misbehaving Nodes in MANETs", iiWAS2010, 8-10 November, Paris, France, pp. 216-222, 2010.

[6] Praveen, J , "Security issues in routing protocols in MANETs at network layer", WCIT, Procedia Computer Science, pp.954-960, 2010.
[7] Sergio, M, Giuli, TJ, Kevin, L & Mary, B, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of Sixth ACM Annual International Conference on Mobile Computing and Networking (MOBICOM 00), Boston, USA, pp. 255-265, 2000.
[8] Hao, Y, James, S, Xiaoqiao, M & Songwu, L, "SCAN: Self-Organized Network-Layer Security in Mobile ad hoc networks", IEEE Journals on Selected Areas in Communications, vol. 24, no. 2, pp. 261-273,2006.
[9] Sanjay, KD, Mohammad, SO, Karan, V, Pushkar, G & Pravina, D "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE SYSTEMS JOURNAL, vol. 5, no. 2,pp.176-188, 2011
[10] Zhi, L, Venkat, N, Amiya, N, & Ivan, S, "Autoregression Models for Trust Management in Wireless Ad Hoc Networks", IEEE Globecom 2011 Proceedings, DOI:10.1109/ GLO COM.20011. 6133993, pp.1-5.
[11] Soufiene, D, Farid, NA, Zonghua & Zhang, 2011, 'Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges', IEEE Communications Surveys & Tutorials,13, no. 4, pp. 658-672, 2011.
[12] Hui, X, Zhiping, J, Xin, L, Lei, J & Edwin, HMS 'Trust prediction and trust-based source routing in mobile ad hoc networks', Ad hoc networks, Elseiver, vol. 11, no. 7, pp. 2096-2114,2013.
[13] Janvon, M, IanWelch, N & Winston, KGS 2012, 'Security threats and solutions in MANETs: A case study using AODV and SAODV', Journal of Network and Computer Applications, vol. 35,pp. 1249–1259.
[14] Gomez, J, Rangel, V & Lopez-Gurrero, 2011, 'NARD: Neighbor-assisted route discovery in MANETs', Wireless Networks, vol. 17, no.8, pp.1745–176,2011.
[15] Govindan, K & Mohapatra, P 2012, 'Trust Computations and Trust Dynamics in Mobile Ad hoc Networks: A Survey', IEEE Communications Surveys and Tutorials, vol. 14, no.2, pp.279-298, 2012.
[16] Venkataraman, R, Pushpalatha, M & Rama, RT 2013, "Regression-based trust model for mobile ad hoc networks," IET Information Security. doi: 10.1049/iet-ifs.2011.0234, pp. 131-140,2013.
[17] Robert, BG, "Exponential Smoothing for Predicting Demand", Cambridge, Massachusetts: Arthur D.Little Inc. pp.97-116,1956.
[18] Robert, BG , "Smoothing Forecasting and Prediction of Discrete Time Series, Englewood Cliffs, NJ: Prentice-Hall,1963.
[19] Charles, C, "Forecasting Trends and Seasonal by Exponentially Weighted Averages", International Journal of Forecasting, vol. 20, pp.5-10,1957.
[20] Winters, PR, "Forecasting Sales by Exponentially Weighted Moving averages", Management Science, vol. 6, no.3, pp.324-342,1960.
[21] Revathi, S & Rangaswamy, T.R., "Dynamic Route Shortening and Route Repairing Mechanism for Mobile Ad Hoc Networks", Journal of Computer Science, Vol. 8, No.8, pp.1212-1218, 2012.

**AUTHORS PROFILE**

**Dr.S. Revathi,** is currently working as an Associate Professor in the Department of Computer Science and Engineering at B.S.Abdur Rahman University, Chennai - 48. She has published 4 research papers in International Refereed Journals and presented one paper in International IEEE Conference. Her areas of interest are Mobile Ad Hoc Network, Network Security, Data Structures and Analysis of Algorithms, Compiler Design.

**Dr. T.R. Rangaswamy** is Professor of Electronics and Instrumentation Engineering Department at B.S.Abdur Rahman University, Chennai, India. He is also acting as Dean(Academic Affairs) at B.S.Abdur Rahman university. He has published more than 40 peer reviewed journal and conference papers in the domain of Automation and Controls, Network Security, Testing, Cyber Security, Modeling and Simulation, RFID and MANET.