Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 02 Issue 02 - 2021 (July to December)

Page 06:11

Improved Routing and Secure Data Transmission in Mobile Adhoc Networks Using Trust Based Efficient Randomized Multicast Protocol

Dr.Nalini Kanta Sahoo
Physics and Chemistry;Life Science and Mathematics
SRM Institute of Science and Technology,Delhi-NCR Campus
ORCHID ID-0000-0002-8804-626X
sahoo.nalini@gmail.com

Article History

Received: 15 July 2021
Revised: 20 September 2021
Accepted: 22 November 2021

Abstract

There is growing concern regarding secure data transfer due to the use of Mobile Adhoc Network (MANET) in many forthcoming technologies and applications.This research proposed novel technique in improving routing and secure data transmission for mobile AdHoc network. here the secure routing is improved using trust based efficient randomized multicast protocol.The protocols can therefore be used with a variety of network designs. The main conclusions of the proposed study are that the token generation method provides improved routing security from a wide range of attacks when coupled with link legitimacy. A node cannot alter its ID while a network is active under the suggested system.Experimental analysis is carried out in terms of throughput, energy efficiency, packet delivery ratio, Message delivery fraction (MDF), end-end delay.

Keywords: MANET, secure routing, secure data transmission, multicast protocol, network lifetime

1. Introduction:

A group of two or more nodes with wireless networking and communication capabilities makes up a MANET. The nodes that are in radio range with one another can speak right away. With aid of intermediary nodes, where packets are forwarded from source to destination, nodes that are not within each other's radio range can communicate [1].To guarantee that packets are successfully routed using a MANET's routing protocol, each node should be setup with a distinct identity. MANETs have a number of benefits over traditional networks, including the ability to be quickly set up and taken down, the ability to provide communication in locations where installing fixed infrastructures is not an option due to factors like location, cost, etc., and the ability to be deployed in an emergency (such as a rescue mission) [2].A node needs authentication to share information securely and to guard against security risks [3]. But because of the following problems, creating secure communication in a MANET is a particularly difficult task: (a) shared wireless medium; (b) no obvious line of defence; (c) self-organizing and dynamic network; (d) the majority of messages are broadcast; (e) messages travel hop-by-hop; and (f) nodes are constrained in terms of computation and battery power [4].

2. Related works:

Several different sorts of study have been done in the last few decades to enhance multipath routing in MANET networks [5]. An energy-centric multipath routing protocol (EMRP), which makes use of data from the physical and Medium Access Control (MAC) levels, was developed in [6].To reduce the chance of link failure in MANETs, the authors of [7] have suggested a Smooth Mobility and Link Reliability-based OLSR (SMLR-OLSR) routing strategy. In order to address the scalability problems frequently connected with the fat routing method in ad-hoc wireless networks, the authors of [8] proposed a variant of OLSR known as Heterogenous OLSR (H-OLSR) routing system.A Q-AODV protocol was suggested in Work [9] to choose a non-congested route based on queue vacancy parameter. An improved Ant-AODV protocol for MANET route selection was put out by the author in [10]. The EMAODV protocol was proposed in work in [11] as a means of controlling congestion. To prevent flooding of RREQ packets, this protocol uses the TTL parameter.

3. System model:

This section discuss novel technique in improving routing and secure data transmission for mobile AdHoc network. here the secure routing is improved using trust based efficient randomized multicast protocol. As a result, the protocols are applicable to a wide range of network architectures.Figure 1 shows proposed architecture.

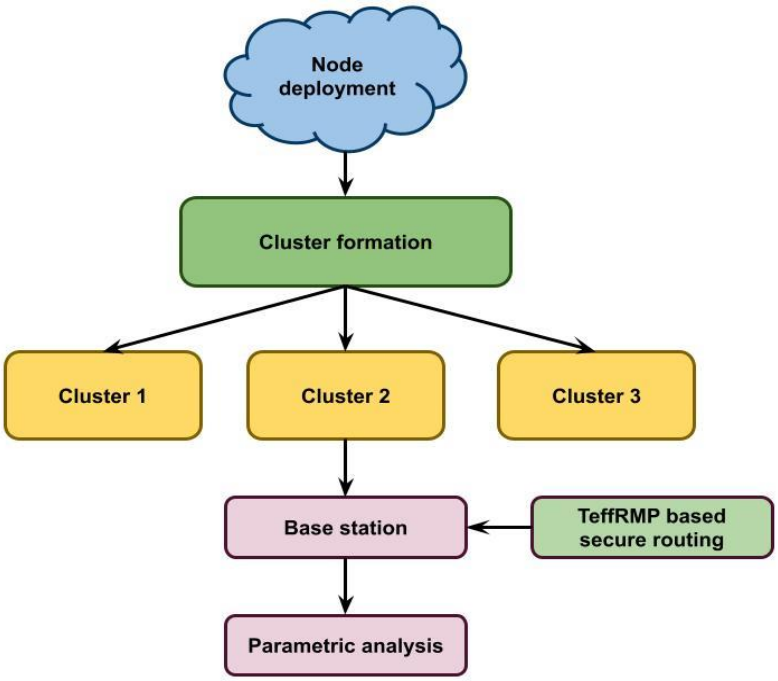

Figure 1: Overall architecture

3.1 Trust based efficient randomized multicast protocol:

In this section, we'll suppose that node A has two different kinds of self-generated RSA-based key pairs: (1) public ((NA; eA))/private (dA) key pairs for message verification and signature; and (2) public (PKA)/private (SKA) key pairs for message encryption and decryption. Here, the secure one-way hash function is used to construct the node identification IDA of node A from its public key ((NA; eA)) (H). Extraction of the link's related security information is the first stage in the link verification procedure. The private key is calculated by the recipient node by eq. (1).

$$\lambda_{\text{receiver}} = \text{hash}(\text{ID}_{\text{receiver}} \parallel t_s) \quad (1)$$

The private key produced by leader node LN is highlighted in expression (2). The technique for evaluating the authorisation key, which is produced as follows:

$$\tau_{\text{receiver}} = \text{generator}r \qquad (2)$$

Receiver node's security validation token (SVT) is calculated over the ciphered data as eq. (3):

$$svt = ct.\lambda_{\text{receiver}} + r_{\text{receiver}} \text{ . generator} \qquad (3)$$

To prevent anyone other than the usual receiver node from testing the validity of the link, the svt is integrated into the data. The receiver node evaluates the authenticity of the link as the process's last phase. After that, the receiving node performs more computation by eq. (4):

$$\text{Generator}_{\text{receiver}} = \text{A. e(B-generator public)} \quad (4)$$

If this requirement is not met, all communication with this link is terminated, and a new link is looked for. For example, k1 and k2 are two trustworthy qualities that are used in the computation of the receiver node's private key, where k1 is equivalent to randomly chosen generator from multiplicative group and k2 is defined mathematically as eq. (5):

$$k_2 = \text{rand}_{\text{receiver}} + \text{hash}(k_1, \text{ID}_{\text{receiver}}) \cdot \text{B} \qquad (5)$$

A random assortment of portable receiver nodes makes up the first component. In contrast, the second component's variable B stands for the pairing parameter's modulus and a random natural integer. The following formula is used to calculate how node I travels toward node j eq. (6):

$$V_{uijd}(\tau + T) = \frac{s(c,\tau) - s(c,\tau - T)}{T}$$
$$IRV_{\omega j\rho}(\mathrm{r} + T) = \frac{1}{T}\left(\int_1^{t-T} \left|V_{wj}(\mathrm{r})\right| d\mathrm{t}\right)$$
$$IRV_{(i,j}(\tau) = \frac{\sum_{i=1,i=1}^{N} N(Is(c,\tau) - s(c,\tau - T)]}{\sum_{i=1}^{N} \frac{NIN-1)}{2} \times T} \qquad (6)$$

N is used to represent all of the nodes in a network numerically. The network's node pairs' relative velocities make up the nodes' relative velocities. The average IRV of nodes may be calculated as bellows, based on fact that mobile nodes regularly change locations at any one time by eq. (7).

$$IRV_{(i,j)}(\tau) = IRV_{(i,j)}(\tau) \times \eta + IRV_{(i,j)}(\tau - T) \times (1 - \eta)$$

$$r_s(i) = \begin{cases} \max\{r_s(i-1) - \alpha, r_s^{thr}\}, & \text{if a piece is lost} \\ \min\{r_s(i-1) + \beta, r_s^{\max}\} & \text{, if a pieccis received} \end{cases} \qquad (7)$$

$$\beta s_l - \alpha l + d \geq 0$$

Even for routes that were completely operational for a lengthy period of time and had ratings that reached their maximum permitted value, rs max, the detection of route failures should be quick.In that case, the failed route would be discarded after at most $f = \left\lceil \left(r_s^{\max} - r_s^{thir}\right)/\alpha \right\rceil$successive failed transmissions. The attacker can choose any l packets to drop undetectedly out of any number of successfully received packets, s, that were permitted to reach the target. It is obvious that from Eq. (8), (using 0 and 0) l will be

$$l \leq \frac{\beta}{\alpha}\left(s + \frac{d}{\beta}\right) \qquad (8)$$

Thus, maximum number of dropped packets by eq. (9)

$$l^* = \frac{\beta}{\alpha}\left(s + \frac{d}{\beta}\right) \qquad (9)$$

$$BWL \leq BWL^* = \lim_{s\to+\infty} \frac{l^*}{s+l^*} = \frac{\beta}{\alpha+\beta} \qquad (10)$$

The upper limit for data loss given in Eq. (10) stands apart from the attack strategy. Therefore, a wise choice of and can lessen the effects of an intelligent opponent that remains undiscovered.

4. Performance analysis:

This part describes the results produced by putting the algorithms covered in the previous section to use. The observations were conducted out using MATLAB scripts while accounting for following simulation parameters: i) a number of mobile nodes of 1400; ii) an initialization energy of 10J; iii) the size of message; and iv) a total of 1000 simulation rounds. Mobile nodes are dispersed randomly throughout a simulated area measuring 1000x1000 m2 in the implementation environment.

Table 1: Comparison of existing and proposed method

Parameters	SMLR-OLSR	H-OLSR	IR_SDT_ERMP
Throughput	85	88	92
Energy efficiency	91	95	98
PDR	88	92	96
MDF	55	58	62
End to End delay	41	43	45

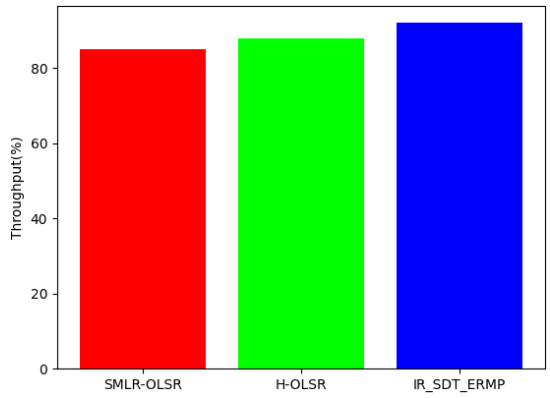

Figure 4: Throughput

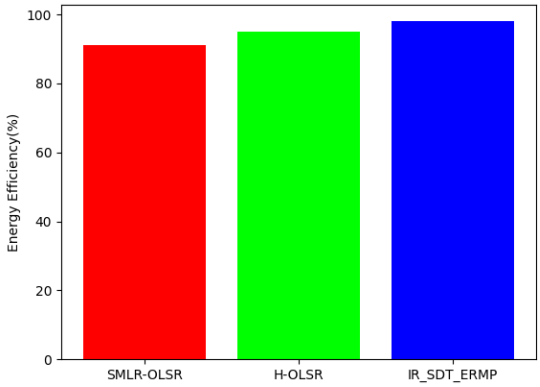

Figure 5: Energy efficiency

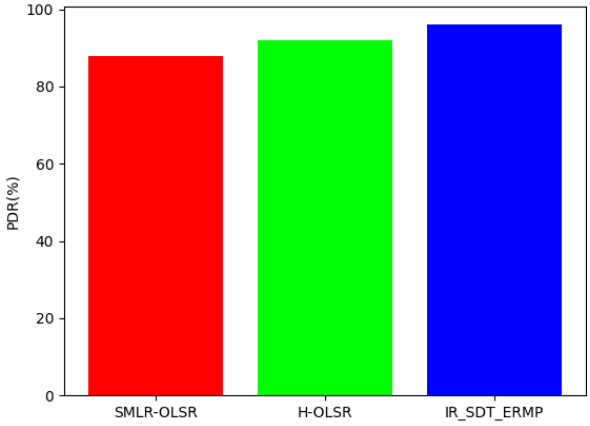

Figure 6: PDR

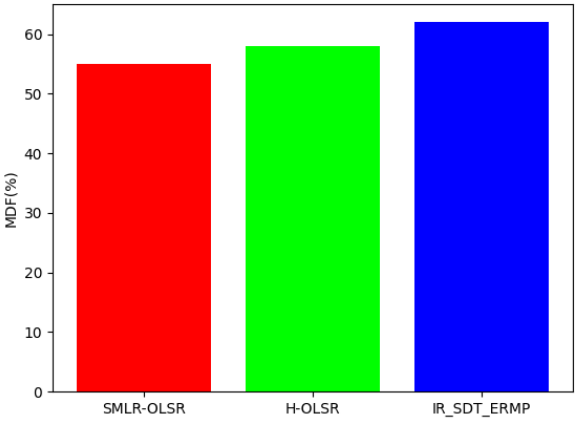

Figure 7: MDF

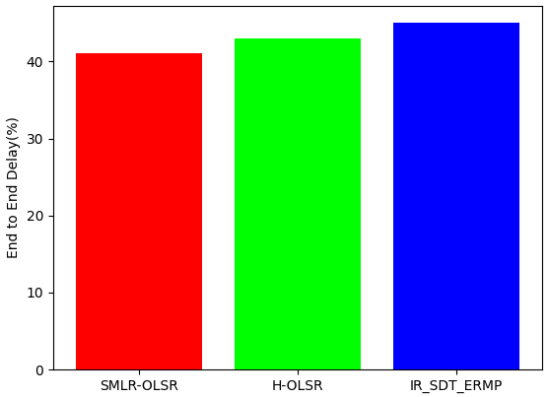

Figure 8: End-End Delay

Throughput of a network is the rate in bits per unit time at which a destination gets data. It is displayed in kbps in figure 4 of the diagram. Proposed protocol has a lower packet delivery ratio than current routing methods, as seen in Figure 5.In comparison to other existing routing systems, Figure 6 shows that suggested routing method exhibits a lower average end-to-end delay. Same is illustrated. Proposed protocol has a higher throughput than existing routing algorithms taken into consideration in this study. Figure 7 compares the proposed and current methods using the message delivery fraction (MDF).Proposed technique energy efficiency is shown in figure8.

5. Conclusion:

This research propose novel technique in improving routing and secure data transmission for mobile AdHoc network. the secure routing is improved using trust based efficient randomized multicast protocol is used for proposed technique. Additionally, this proposed protocol provides multipath routing, which reduces floating of pointless control packets for route establishment under node failure or congestion. Additionally, this protocol maintains secure connection by looking out for hostile nodes. Throughput, energy efficiency, packet delivery ratio, message delivery fraction (MDF), and end-end latency are all considered in the experimental analysis. Proposed technique attained throughput 92%, energy efficiency 98%, packet delivery ratio 96%, Message delivery fraction (MDF) 62%, end-end delay 45%

Reference:

[1] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, “Security challenges and attacks in dynamic mobile ad hoc networks MANETs,” in Proceedings of the JEEIT, pp. 28–33, Amman, Jordan, April 2019.

[2] Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. *IEEE Transactions on Reliability*, *69*(3), 1077-1086.

[3] Bhagyalakshmi and A. K. Dogra, “QAODV: A flood control ad-hoc on demand distance vector routing protocol,” in Proceedings of the ICSCCC, pp. 294–299, Jalandhar, India, March 2018.

[4] D. Sarkar, S. Choudhury, and A. Majumder, “Enhanced-AntAODV for optimal route selection in mobile ad-hoc network,” Journal of King Saud University-Computer and Information Sciences, vol. 8, 2018.

[5] H. Jhajj, R. Datla, and N. Wang, “Design and implementation of an efficient mul- tipath AODV routing algorithm for MANETs,” in Proceedings of the CCWC, pp. 0527–0531, Las Vegas, NV, USA, December 2019.

[6] Rajeswari, A. R., Kulothungan, K., Ganapathy, S., &Kannan, A. (2019). A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. *Peer-to-Peer Networking and Applications*, *12*(5), 1076-1096.

[7] Zhang, D. G., Zhao, P. Z., Cui, Y. Y., Chen, L., Zhang, T., & Wu, H. (2019). A new method of mobile ad hoc network routing based on greed forwarding improvement strategy. *IEEE Access*, *7*, 158514-158524.

[8] M. D. Sirajuddin, C. Rupa, and A. Prasad, "Advanced Congestion Control Techniques for MANET," Advances in Intelligent Systems and Computing, vol. 433, pp. 271–279, 2016.

[9] Robinson, Y. H., Krishnan, R. S., Julie, E. G., Kumar, R., & Thong, P. H. (2019). Neighbor knowledge-based rebroadcast algorithm for minimizing the routing overhead in mobile ad-hoc networks. *Ad Hoc Networks*, *93*, 101896.

[10] Anand, M., &Sasikala, T. (2019). Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol. *Cluster Computing*, *22*(5), 12681-12687.

[11] Arulkumaran, G., &Gnanamurthy, R. K. (2019). Fuzzy trust approach for detecting black hole attack in mobile adhoc network. *Mobile Networks and Applications*, *24*(2), 386-393.