The Finest Secured Routing Techniques with Transmission of Data in Mobile Ad Hoc Networks

R. Nandakumar and K. Nirmala

Abstract In this paper, we proposed the finest secured routing technique in mobile ad hoc network. While sending messages in the MANET, there may be possible various attacks. Signature-based secured routing techniques are proposed in this paper. This routing technique is mainly focused on a dynamic process in the MANET which is classified into two levels of security. These Secured Routing techniques used to determine the generated keys of each and every messages and also authenticated by the source, destination and intermediate node at perfect level. The secured routing techniques in the low level are determined as the normal level; the source node and destination node will authenticate the entire routing process. Hence this paper proposed the finest secured routing techniques in MANET.

Keywords MANET · Secured routing techniques · AODV · Routing protocol

R. Nandakumar (✉)
Computer Science, R V Government College, Chennai, Tamil Nadu, India

K. Nirmala
Quaid-E-Millath Government College for Women (Autonomous),
Chennai, Tamil Nadu, India

A. Ramu et al. (eds.), *International Conference on Computing, Communication, Electrical and Biomedical Systems*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-030-86165-0_10

1 Introduction

MANET might be an arrangement of two or a great deal of nodes outfitted with remote interchanges and system administration capacity. The nodes inside the radio fluctuate and will immediately speak with each other. The Hidden Node which act as an intermediate node to transferred the information to attain objective. Each node composed to a particular information with help of Mobile Adhoc Network.

A Routing protocol mainly classifed into three categories [1]: (a) on demand, (b) table driven, and (c) hybrid routing protocol [2] or a combination of on-demand routing protocol and table-driven protocol. In on-demand routing protocol, each node will find the appropriate route to send the data to the destination node [3]. In on-demand routing protocol, the route to the destination node remains unknown for every intermediate node in MANET. Ad hoc on-demand distance vector and dynamic source routing protocol will be under on-demand routing protocol. The destination-sequenced distance vector (DSDV) [4] is mainly under on table-driven routing protocol.

Zone routing protocol acts as a hybrid of on-demand routing protocol and table-driven routing protocol.

AODV is an on-demand routing protocol [5] mainly considered in this paper [6]. This on demand routing protocol will make the route to the destination nodes very effective. If a flood occurs while sending a data in the appropriate route, the route request message will be passed through the entire network and at the time through the route discovery process. The route reply message will be sent to paths towards the source node. The three types of security threats with AODV are:

(a) Modification attacks which include redirection by the route sequence number, the node count, services denial, and the pipeline process [6]
(b) Identity attack which includes the node that is malicious based on their identity
(c) Fabrication attacks mainly focused on the false route which leads to error messages

2 Literature Survey

An Adhoc System arranged with a mixed portable hubs to determine the unified process in MANET [7]. Every versatile hub goes about as host and switches. Besides, Some of the elective hubs were not used for transmission, in other words all the hubs used in the Adhoc network were not used for transmission [8]. On this paper, a propelled component is given against these empty assaults during a MANET. The existing procedures utilize quality of service (QoS) for the whole system to find assaults. Our philosophy utilizes the bundle conveyance quantitative connection and excursion time for each hub, and it moreover identifies dynamic and aloof assaults. Along these lines, the entire ID of empty assault is a practical exploitation of the arranged procedure.

The possibility Delivery quantitative connection (PDR) boundary worth is misrepresented as demonstrated by the variable alteration of the amount of hubs to be zero.431%, decreasing the regular postponement by sixty three.525%, and assembling the vitality utilization overstated by zero.170% [9]. Recreation [4] with the variable alteration of speed got zero.482% PDR results, decreasing the normal postponement by seventy eight.710% and vitality utilization overstated by zero.167%. Alteration of cushion size factors got zero.729% PDR results, decreasing the regular deferral of seventy one.603% and vitality utilization misrepresented by zero.161%. From these data, MANET AODV-DTN is better than MANET AODV.

[10] expound on the center of the convention and examine the advancement, its variations, expansions, and accordingly the applied thought. We have studied the expansive space of AODV [11] augmentations and have ordered them to bolster the varying standards, e.g., quality, reliability, vitality, security, steering strategies, and so forth. This paper draws out the origination, style objective, examination patterns, and consequently the current progressions inside the investigation controlled for AODV improvement [11]. The paper also sums up various parts of the investigation slants and depicts execution measurements, input boundaries, pertinent spaces, and along these lines the received strategies for up the convention [12].

3 Proposed Architecture

The proposed work is mainly focused on the transport layer of the OSI architecture. This layer is mainly focused on transmission of data from one node to another node. While transferring a data from one node to another node, there may be certain flaws such as data may be lost due to environmental change in the ad hoc networks. This paper is focused on the proposed secured routing techniques while transferring data from one node to another node in the MANET as given in Fig. 1.

From the above diagram, the source node (S) will send a message to the destination node (D). This proposed routing technique is used to determine three types of security level: the source node, intermediate node and destination node.

We had proposed two cases related to the level of securities as described below.

Case 1 This is the perfect level of security of data transmission, during the process of routing. This level of security assumed to be one (level of security = 1). During the process of routing, the source node and destination node separately verify the authentication of all the intermediate nodes in the given routing path. Each intermediate node will authenticate with a neighboring node which includes both previous and next nodes in the given routing path.

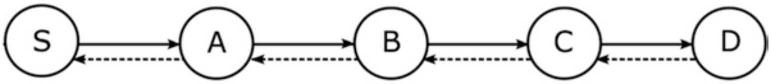

Fig. 1 Process of routing protocol

Case 2 This is the normal level of the security of data transmission, during the process of routing. This level of security assumed to be zero (level of security = 0). During the process of routing, the source node and destination node alone verify and authenticate with each other. Each intermediate node authenticates with the neighboring node which includes both previous and next nodes.

This proposed routing protocol technique is the combination of sequential aggregate signature based on RSA algorithms. It's mainly categorized into two levels: (a) session key generation along with route discovery and (b) maintenance route information.

(a) **Session Key Generation Along with Route Discovery:** This process is done at three levels of nodes such as source node, intermediate node, and destination node at both cases as shown in Fig. 2.

Source node : A prime number, two random numbers generated, encrypts the random number based on the proposed techniques, broadcasts the random number from the source node, and requests the message which consists of source IP address, sequential number of the source, destination IP address, and broadcast ID.

Intermediate node : The intermediate node will check the broadcast and request message from the previous node. Initially, it will check the previous node to be authenticagted and will perform the next process to send the request message, broadcast ID to the next level of intermediate node.

Destination node : The destination node (D) will authenticate all the intermediate nodes and request the source ID, source IP address, and broadcast ID. If all the AODV protocols are true, then it will decrypt the random number and prime number at the destination level. If it fails, the messages will not be authenticated to view at the destination level.

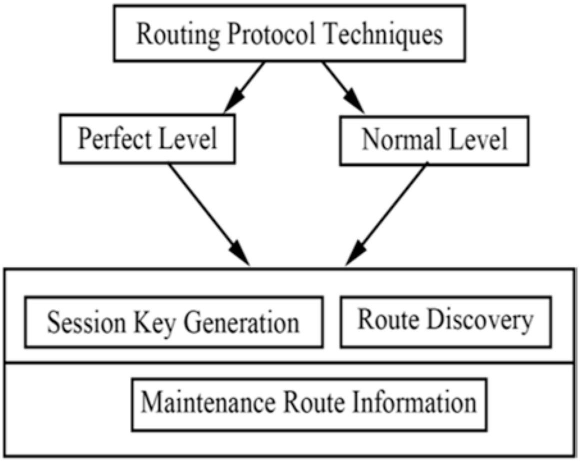

Fig. 2 Proposed routing protocol

(b) **Maintenance Route Information:** This process is used to determine the route information in both cases.

Source node : Broadcast ID, the request message generated at the source node, sends the request message based on AODV to the next node.

Intermediate node : The intermediate node receives the request message from the previous node, it authenticates the request message, it removes the signature message, and it regenerates the broadcast ID to the next level of intermediate node.

Destination node : The destination node checks the information received from the previous intermediate node of the request messages and also checks the entire path of the intermediate node along with the source node.

4 Algorithm and Experimental Result

A Proposed Routhing Adhoc on-demand distance vector (AODV) algorithm described with two cases.

```
// Algorithm
Step 1    Let $p_i$ be the Prime number
Step 2    Let $r_1$ and f be the generate random number of the source node
Step 3    Let $R_1$ be the Generate number based on the mod value of pi to the power of g
Step 4    Let $R_2$ be the encrypted key of r1
Step 5    Sig(S) = $R_2$ key are broadcast with the appropriate id of the source node
Step 6    Req(S) includes ip address,the sequence number of the source, broadcast id, destination address, source address based on the AODV protocol
Step 7    If level is equal to 1
Step 8    {
Step 9    If(k equal to intermediate node)
Step 10   {
Step 11   Each intermediate node will authenticate the request message Req(Previous node) received.
Step 12   Req(Previous node) consist of ip address,source address, sequence number of the source, broadcast id, destination.
Step 13   If(authentication failed) messages will not receive by the destination node
Step 14   else If (k be the destination node)
Step 15   {Destination node will receive the Req(previous node), it will check the appropriate parameters of the source and intermediate node.
Step 16   If(Req (previous node) )
Step 17   The Message received by the destination node
Step 18   else
Step 19   Message failed. }}}
Step 20   If(level ==0)
Step 21   {Source node will generate generate broadcast id, and Req(S) which include ip address, source address, destination address.
Step 22   Each intermediate node receives the Req(Previous node) and remove the signature
          key of the previous node, regenerate the broadcast id and send to the next level of
          node.
Step 23   If the previous node are not authenticate, message will be failed at the existing
          intermediate node
Step 24   Else the message passed to the next level
Step 25   Destination node will authenticate the previous request message, and also the
          source ip address. If both parameter are authenticate, message will be decrypt and
          leads success routing process.
Step 26   Else message are failed in the normal level.
}
```

Security and Performance Analysis Figure 3 presents the process of the proposed routing techniques for both perfect level and normal level.

Security Level The performance analysis is mainly focused on the security level based on the two cases: (a) perfect level and (b) normal Level. The following table is generated with the sample node for both of the cases.

From the Table 1, the following graph generated which result the security level of proposed techniques. The graph presents the perfect level which will lead to be more effective compared to the normal level in Fig. 4.

Message Delivery Ratio The message delivery ratio is determined by the total number of messages received divided by the total number of messages transmitted at a particular node in the routing path. The proposed routing techniques are compared with the existing routing techniques using MANET. The following table is generated with the sample data compared with the existing one with proposed routing techniques as shown in Fig. 5.

The following graph is generated from Table 2 which provide the performance analysis of the existing algorithm with proposed AODV in MANET.

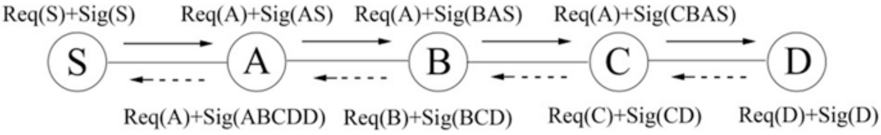

Fig. 3 Process of proposed routing techniques in MANET

Table 1 Security level

Level/node	75	50	25
Perfect	92.00	93.33	93.85
Normal	89.33	90.67	92.31

Table 2 Security level

	Received	Transmitted
AODV	88.67	87.33
PAODV	92.67	90.67

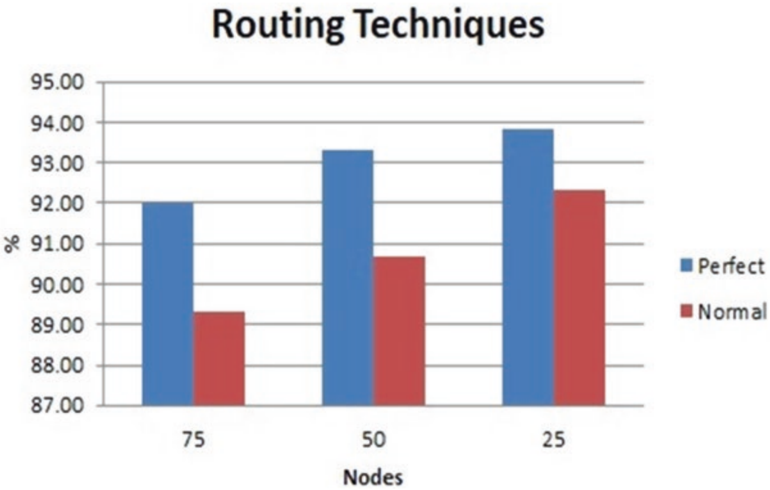

Fig. 4 Security level

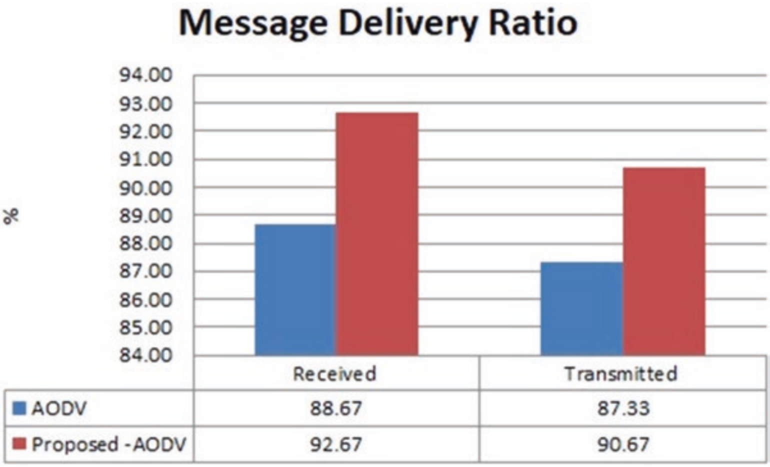

Fig. 5 Message delivery ratio

5 Conclusion

It is concluded that this paper focused on the MANET using ad hoc on-demand distance vector (AODV) protocol is used to improve the routing techniques based on the security level of the messages sent and received by the source node, intermediate node, and destination node. This paper also proposed two levels of security, such as perfect level and normal level, with automated key generation based on the public and private key. This proposed security and routing techniques with transmission of data in MANET are determined to be effective and efficient.

References

1. Abhilash, K.J.: Secure routing protocol for MANET: a survey. In: Advances in Communication, Signal Processing, VLSI, and Embedded Systems, pp. 263–277. Springer, Singapore (2020)
2. Ahlawat, B.A.: Performance analysis of congestion control in MANET using different routing protocols. Int. J. Comput. Sci. Eng. **7**(7), 312–319 (2019)
3. Manikandan, R.M.: A literature survey of existing map matching algorithm for navigation technology. Int. J. Eng. Sci. Res. Technol. **6**(9), 326–331 (2017)
4. Choudhary, D.: Performance optimization by MANET AODV-DTN communication. In: Soft Computing: Theories and Applications, pp. 1–9. Springer, Singapore (2020)
5. Ghosh, W.: Secure routing and data transmission in mobile ad hoc networks. Int. J. Comput. Netw. Commun. **6**(1) (2014)
6. Goyal, A.S.: Modified local link failure recovery multicast routing protocol for MANET. J. Inf. Optim. Sci. **41**, 669–677 (2020)
7. Nages Wadhwani, G.K.: Trust framework for attack resilience in MANET using AODV. J. Discret. Math. Sci. Cryptogr. **23**, 209–220 (2020)
8. Sakthivel Nageshwaran, S.D.: Optimization techniques in network slicing and human approach for education game. In: 4th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 318–323. IEEE (2020)
9. Sankara Narayanan, S.: Modified secure AODV protocol to prevent wormhole attack in MANET. Concurr. Comput. Pract. Exp. **32**, e5017 (2020)
10. Soni, G.: Multipath location based hybrid DMR protocol in MANET. In: 2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), pp. 191–196 (2020)
11. Saini, T.K.: Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. Ad Hoc Netw. **103**, 102148 (2020)
12. Zare, H.: Effective congestion avoidance scheme for mobile ad hoc networks. J. Comput. Netw. Inform. Secur. pp:33–40 (2013)