Load Based Key Generation for MANETs with DSR and AODV Routing Techniques

Shibu K.R, Suji pramila R

***Abstract:** Automatic key establishment schemes are the root of secure communication in Mobile adhoc networks(MANETs). These schemes are not universal; their performance depends on many factors like routing protocols, type of attackers aimed at, the parameter used for key generation, etc. Among the routing protocols used in MANETs the most popular ones are reactive routing protocols DSR and AODV. In this paper, an efficient secret key establishment technique using traffic matrix is simulated in the two reactive routing protocol scenarios: DSR (Dynamic Source Routing) and AODV (Ad hoc On-demand Distance Vector routing). The simulation results are compared and analyzed in terms of the key generation complexity, packet loss ratio and active attacker detection. Finally the paper concludes the fact that traffic load based key generation scheme is preferable for reactive routing protocol based systems.*

Keywords: DSR, AODV, Traffic matrix, Secret key

I. INTRODUCTION

MANETs are a group of dynamic mobile nodes without specific infrastructure and base stations. The wireless nodes in the network are free to act as a source or destination at any time. This inherent nature of MANETs makes them popular in many important communication applications including military applications. The lack of centralized authority makes these networks more prone to security issues. So there is a growing need in data security management in MANETs. To address these security issues various secret key generation techniques are deployed. However, the applicability of the common key generation schemes to the network depends on many factors [1] including routing strategies, nature of network, etc. Also, many of the existing key generation schemes find it difficult to identify a suitable randomness source [2] for key generation.

The kind of network that utilizes on-demand reactive routing protocols is maintaining a route table at the node level. The routing information thus stored helps them in finding routes each time the nodes want to communicate in the future. The details stored in the nodes are highly dynamic and unpredictable; this ensures a truly random set of data for randomness extraction [3]. Data traffic in the network can also be recorded and utilized as another randomness source. Mostly the traffic volume is maintained in the matrix form at each node. The traffic matrix based secret key generation scheme exploits the fact that several system metadata can be deployed to extract secret keys in MANETs. The scheme is extracting the randomness source from the system metadata: the traffic load and the routing table. This type of key generation is applicable for MANETs that are using reactive routing protocols [4].

In this paper, the target is to simulate the traffic matrix based key generation scheme for the two different reactive routing protocols DSR and AODV [5]. The results of the two are compared to identify the suitability of the proposed scheme. The paper is organized as follows: The brief review of the related works is given in section 2. Section 3 presents the reactive routing protocol review based on DSR and AODV. Section 4 discusses the traffic matrix based random bit extraction and section 5 outlines the simulation results. Finally, section 6 concludes the paper.

II. RELATED WORKS

Many techniques were developed to protect MANETs from intruders. But the inherent nature of adhoc networks makes them more vulnerable to attacks. Also, the traditional routing algorithms will not work well for this kind of network. The majority of the key management schemes work in association with the routing protocols.DSR and AODV are routing protocols designed to use in adhoc networks.

DSR and AODV based communication needs two levels of security: the source authentication and message validation. The attackers in the network can affect adversely by imitating the source node, altering the sequence number creating routing loops and also by creating inconsistency in the network.

In [6] survey on the reactive routing protocols outperforms the non reactive routing protocols as the size of the network increase. It shows the performance of these protocols in a simulated adhoc environment. Also, various key management schemes are utilizing those routing protocols for key generation.

Usman et [7] al proposed a dynamic method for securing the data in adhoc networks, for that they used a symmetric encryption approach which will act as a framework for security. But the cost incurred in the encryption procedure is high. In this, a handshaking approach is used for node communication. This is a noticeable work in the field of adhoc networks. The storage requirement will increase based on the number of nodes.N Alangudi [8] et al proposed an enhanced key generation method for vehicular networks, which is a modified version of ECC and Diffie-Hellman key exchange algorithm. It has been proposed to work out routing overhead and the delay in communication. The dual authentication technique proposed here decreases the time for key generation and also the secrecy is maintained efficiently. The main concern here is the key updating delay.

Revised Manuscript Received on February 15, 2020.

Shibu K .R*,Research Scholar, Computer science engineering Department, Noorul Islam Centre For Higher Education, Kumaracoil , Thucklay , Tamilnadu, India. Email: shibukarakkattu@gmail.com

Suji Pramila R,Associate Professor, Computer science engineering Department,Noorul Islam Centre For Higher Education, Kumaracoil, Thucklay, Tamilnadu, India.Email: sujisymon@gmail.com

Retrieval Number: C4752029320/2020©BEIESP
DOI: 10.35940/ijeat.C4752.029320

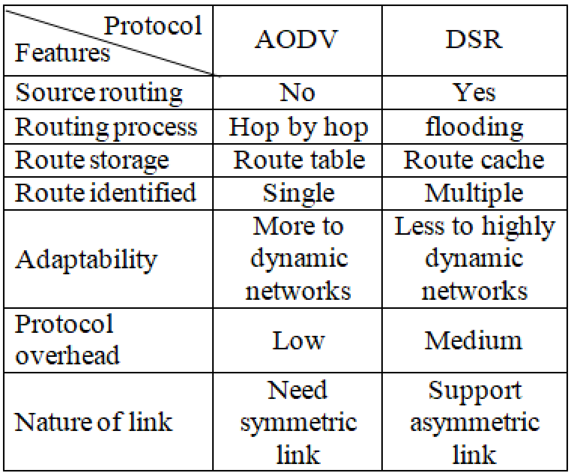
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In [9] an exceptional classification on the types of attacks in adhoc networks is carried out. Also clearly distinguished active and passive attacks along with a comprehensive analysis of the existing intrusion detection techniques and their processing capabilities are surveyed. The paper highlights the fact that intrusion detection is very essential for secure communication.

III. REACTIVE ROUTING PROTOCOLS AND THEIR CHARACTERISTICS.

Several routing protocols [10] are available in MANETs which come the three main categories: proactive, reactive and hybrid protocols. Among these, the reactive protocols are the most accepted ones as they have the lowest routing overhead and bandwidth requirement. These protocols use broadcast based methods for route identification according to their communication demand. In broadcast based routing the source node initiates the route identification process by sending a route request packet RREQ to all the neighboring nodes. This packet traverse through the network until an intermediate or destination node responds by sending a route reply packet RREP back to the source node. Once the route is identified the route details are cached at the nodes for further communication. In this study, we have selected on demand reactive routing protocols AODV and DSR because they have some similarities [11] which make them suitable for the proposed secret key generation scheme. The table I list out the similarities and differences that account in our studies.

Table- I. AODV vs DSR



Protocol Features	AODV	DSR
Source routing	No	Yes
Routing process	Hop by hop	flooding
Route storage	Route table	Route cache
Route identified	Single	Multiple
Adaptability	More to dynamic networks	Less to highly dynamic networks
Protocol overhead	Low	Medium
Nature of link	Need symmetric link	Support asymmetric link

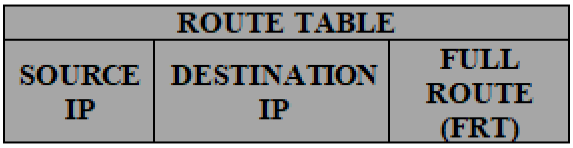
The major difference between the two is that in DSR the nodes maintain the full route details of all the communication whereas in AODV nodes store only the net hop information. To implement the traffic matrix based scheme in AODV the full route details are stored at each node. Also, the additional factor needed is the maintenance of the traffic matrix which can be done utilizing the traffic volume information.

IV. SECRET KEY GENERATION

Mostly MANETs are used in situations where the information needs utmost confidentiality and security. As MANETs are an autonomous group of nodes without any infrastructure they are highly vulnerable to attacks. So a lot of attack prevention techniques like encryption, random secret key generation, etc are designed to address these issues. But the majorities of the existing techniques are either very complex in computation or are not able to identify a proper randomness source for key generation. In the scheme proposed here, a two factor authentication is ensured by using two different system metadata, the routing information, and traffic load.

A. Routing Information

To route both DSR and AODV are maintaining a routing particular in the form of tables at each node. The route table record includes the details of the source and destination nodes of each data transfer, the RREQ ID number and the full route details. This information is updated each time an RREQ is received or a data packet passes through the node. The routing information is stored in the form of a table as shown in Fig 1 at individual nodes.

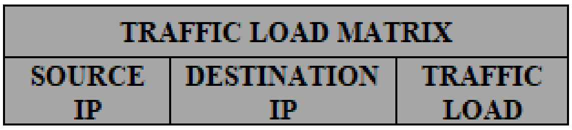


ROUTE TABLE		
SOURCE IP	DESTINATION IP	FULL ROUTE (FRT)

Fig 1.Routing information

B. Traffic Load Matrix

The traffic matrix is a two dimensional matrix created and maintained at every node (p) in the network for implementing the proposed key generation scheme. The main contents of the traffic matrix are given in Fig. 2. The matrix is an N x N matrix for a system where 'N' is the maximum number of nodes in the network. The entries in the matrix are the cumulative traffic volume of the node for a particular source-destination pair. The traffic volume refers to the number of data packets moving through the node at any instant of time.



TRAFFIC LOAD MATRIX		
SOURCE IP	DESTINATION IP	TRAFFIC LOAD

Fig 2.Traffic matrix entry format

The row value indicates the source ID (S_i) and column value gives the Destination ID (D_j). The traffic load (L_{ij}) is defined as the cumulative number of data packets send from a source 'Si' to the destination node 'D_j' in the network. The complete traffic matrix for a node 'P' is given in the Fig.3;

$$\mathbf{TLM\,(p)} = \begin{array}{c|cccccc|} & \mathbf{D1} & \mathbf{D2} & . & . & . & \mathbf{D_N} \\ \hline \mathbf{S1} & L_{11} & L_{12} & . & . & . & L_{1N} \\ \mathbf{S2} & L_{21} & L_{22} & . & . & . & L_{2N} \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ \mathbf{S_N} & L_{N1} & L_{N2} & . & . & . & L_{NN} \end{array}$$

Fig 3.Traffic matrix

Each entry in the matrix can be given as a summation of the total number of data packets transfer between the source-destination (i ,j) pair through the node 'P' which is transmitted through full route R_p;

$$L_{ij}(p) = \sum N(S_i,D_j; R_p) \qquad \forall\ N(S,D) \in R_p \quad (1)$$

Where, N(S, D ; R) is the traffic volume going from ‘S’ to ‘D’ through route ‘*R’* which includes node ‘p’. The entries are updated each time a packet passes through the node ‘p’. This ensures that the data stored in the matrix are random enough to be used for secret key generation.

C. Randomness Source

The primary requirement for any secret key generation scheme is a set of truly random and identical data at the two communicating nodes. The source and destination nodes initiate the key generation by extracting this set of random data that are unique and identical at these nodes. The data stored in the traffic matrix along with the routing data stored in each node is used for randomness source extraction. When node ‘p’ wants to communicate with another node ‘q’ the data extraction at these nodes can be explained using the following algorithm: Random bit extraction Algorithm at node ‘p’:

Step1: The node ‘p’ is assigned as the source node and node ‘q’ as the destination.

Step2: Node ‘p’ checks its routing table for full route entries (FRT) with ‘p’ and ‘q’ as intermediate nodes and create SD (source-destination) pair list 1.

$$SD1\ [\ ] = S_iD_j(p,q) \in FRT(p)$$

Step 3: Go for a second iteration and identify whether any of the identified SD pair exists in the full route table such that only node 'p' is coming as an intermediate node.

$$SD2\ [\ ] = \{S_iD_j(p) \in SD1[\ ]\ \}\ \&\&\ \{S_iD_j(p) \in FRT(p)\ \}$$

Step 4: Get the difference of the two sets

$$SD\ [\ ] = SD1\ [\ ] - SD2\ [\ ]$$

Step 5: Extract the traffic load entries from the TLM corresponding to each SD pair

$$TL\ [\ ] = \text{for all } SD\ [\ ]\{\ L_{ij} \in TLM(p)\}$$

Step 6: TL [ ] is the randomness source data

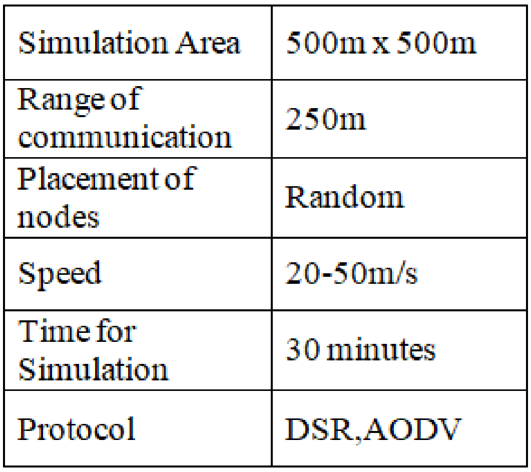
Step 7: Assign binary bits to each entry in TL [ ] matrix. XOR the binary numbers to generate random bits.

The same algorithm can be applied at node ‘q’. Extracted random bits will be identical. The system can generate a set of random bits with the extracted traffic load value. The number of bits can be decided based on the level of security needed. The higher the numbers of bits more secure the generated key.

V. EXPERIMENTAL RESULTS AND ANALYSIS

The secret key generation based on the traffic load details is simulated in NS2 with the DSR and AODV protocols. The simulation environment had the parameters as given in Table II. The two schemes have their own unique features, so the results were different for the two. The comparison is done based on three features: Key generation delay and computational overhead, Average packet loss ratio, Active attacker detection.

Table -II. Configuration Followed For Simulation



Simulation Area	500m x 500m
Range of communication	250m
Placement of nodes	Random
Speed	20-50m/s
Time for Simulation	30 minutes
Protocol	DSR,AODV

A. Key generation delay and computational overhead

As mentioned in section 3 the two protocols have a slight difference in the method of saving routing details for route identification even though both are using flooding mechanisms. AODV is saving the next hop details whereas the DSR is saving the full route details at each node after every route identification process. So for our scheme of key generation, the DSR is more suitable. To implement the proposed scheme an additional overhead of creating and saving routing details is needed for AODV. But as the system is already saving the next hop details, the additional memory requirements are very less. The total time taken to find out the randomness source can be given as the sum of time taken to list out the SD pair list from the FRT (p) and the time taken to identify the traffic load values from the TLM(p).

$$T_{avg} = f\,(\text{SD pair extraction time} + \text{Traffic load data extraction})$$

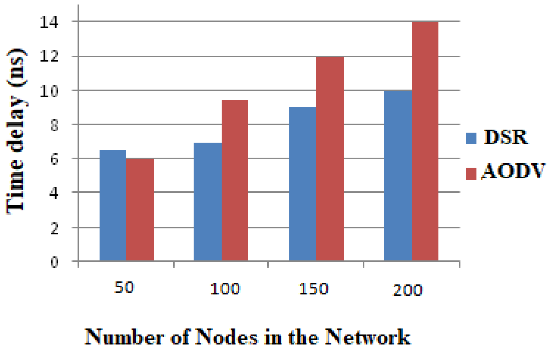


Fig 4.Time delay vs Number of nodes

The result in the Fig.4 shows that the time delay is lower for the network with a lower number of nodes. In small networks, the AODV is found more efficient but for larger networks, the DSR based scheme is more time efficient.

B. Packet delivery Ratio

Packet delivery ratio is the quantitative relation between the number of data packets reached at the target node to the total number of data packets transmitted by the source node. This ratio depends on many system factors like the routing strategy, rerouting in case of route beak up, mobility of nodes, presence of malicious nodes [12], etc.

Despite the fact that DSR and AODV are reactive routing protocols their strategic method of handling erroneous routes is different [13]. Basically, DSR is considered more efficient to redirect a data packet through another existing route to the destination if there occurs a route breakup. Also, both protocols do not have intrinsic security or defensive mechanism.

The simulation was done assuming that the mobility of the nodes is minimum so that route breaks up and rerouting possibilities are minimum. The efficiency of the secret key generated is tested with varying number of malicious nodes in the system. The simulation is done with two different key generation schemes: simple random number generator and traffic load based key generation. The results are shown in Fig 5.

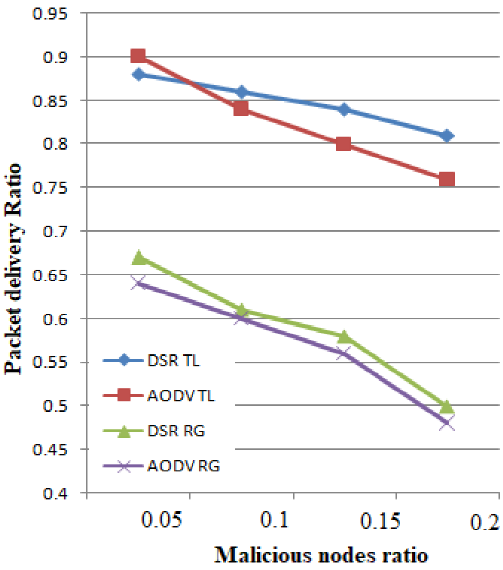


Fig 5. Impact of malicious nodes on packet Delivery

As expected the packet delivery ratio was higher when the traffic load based key was used. The second point noticed here is that the packet delivery ratio is almost constant for the DSR whereas for the AODV the ratio is decreasing with an increase in the number of malicious nodes

C. Active attacker detection

In general, the attackers in the MANETs are grouped into two: 1) passive, those malicious nodes which do not take part in communication but tries to overhear the information 2) active, they actively take part in the communication either by sending a false message or by modifying them. The recent works are mainly concentrating on the detection or prevention of passive attackers by using suitable key generation techniques.

As discussed earlier, the proposed system creates and maintains a traffic load matrix for extracting random bits for the secret key generation. Exploiting this stored information for active attacker detection is the main attraction of the proposed scheme. The recent research works [14-16] shows that an active attacker always tries to track the data communications in the network. Active attackers also become part of the major routes [17] to take part in the communication.

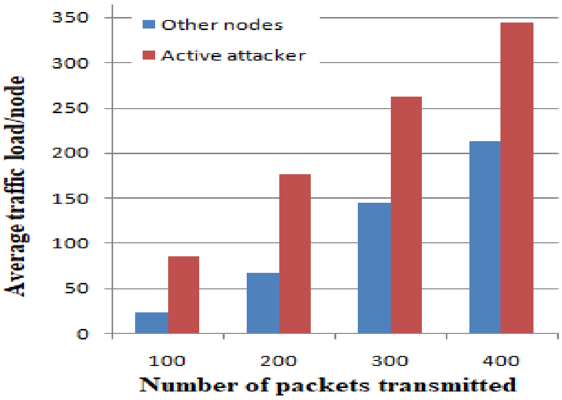


Fig 6.Avg traffic load vs Number of Packets

In the TLM(p) maintained by the node 'p' the count of the number of data packets passing through the node between all the node pairs is available. If a node suspects another node ‘aa’ as an active attacker it can identify the same in two steps: 1) search its own full route table and if the number of full routes in which ‘aa’ is an intermediate node is greater than ¾ of the total number of routes in the table and 2) find out the average of the traffic load entries ‘L_{ij}’ in which ‘aa’ is an intermediate node. If both are found to be high then the probability that node ‘aa’ is an active attacker is maximum. The Fig.6 shows that the active attacker tries to become part of all most the active routes and the average traffic load value is very high for the active attacker node.

VI. Conclusion

Considering the importance of MANETs in various applications that require a high level of security, in this paper a new key generation scheme is simulated in two different scenarios. It is observed that the key generation scheme suites for reactive routing protocol based networks. Even then the performances vary and DSR outperforms the AODV in many situations like key generation speed, packet delivery loss, and memory requirement. The scheme is found highly successful in identifying active attackers in the network without much extra computational overhead. Thus the traffic matrix based key generation scheme provides a secure key management scheme that can be integrated with reactive routing protocols.

REFERENCES

1. Sarangapani, J. (2017). Wireless ad hoc and sensor networks: protocols, performance, and control. CRC Press.
2. Shibu, K. R., & Pramila, R. S. (2019). Random Bit Extraction for Secret Key Generation in MANETs. Wireless Personal Communications, 1-15.
3. Nayyar, A., & Mahapatra, B. (2020). Effective Classification and Handling of Incoming Data Packets in Mobile Ad Hoc Networks (MANETs) Using Random Forest Ensemble Technique (RF/ET). In Data Management, Analytics and Innovation (pp. 431-444). Springer, Singapore.
4. Darabkh, K. A., & Judeh, M. S. (2018, June). An Improved Reactive Routing Protocol over Mobile Ad-hoc Networks. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 707-711). IEEE.
5. Shivahare, B. D., Wahi, C., & Shivhare, S. (2012). Comparison of proactive and reactive routing protocols in mobile adhoc network using routing protocol property. International Journal of Emerging Technology and Advanced Engineering, 2(3), 356-359.
6. Baby, B., & Pramila, R. S. (2018). Survey on analysis of energy optimization in MANET routing. International Journal of Engineering & Technology, 7(3), 1951-1955.

7. Usman, M., Jan, M. A., He, X., & Nanda, P. (2018). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems.
8. Balaji, N. A., Sukumar, R., & Parvathy, M. (2019). Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network. Computers & Electrical Engineering, 76, 94-110.
9. 9.Kumar, S., & Dutta, K. (2016). Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. Security and Communication Networks, 9(14), 2484-2556.
10. Shibu, K. R., & SujiPramila, R. (2018). Routing protocol based key management schemes in manet: a survey. International Journal of Engineering & Technology, 7(3), 1453-1456.
11. A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure and P. Spilling.(2006) A survey of key management in ad hoc networks, in *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 48-66, 3rd Qtr. 2006
12. Kang, N., Shakshuki, E. M., & Sheltami, T. R. (2010, November). Detecting misbehaving nodes in MANETs. In Proceedings of the 12th international conference on information integration and web-based applications & services (pp. 216-222). ACM.
13. Shrivastava, L., Bhadauria, S. S., & Tomar, G. S. (2011, June). Performance Evaluation of Routing Protocols in MANET with different traffic loads. In 2011 International Conference on Communication Systems and Network Technologies (pp. 13-16). IEEE.
14. Liang, Y., Poor, H. V., & Ying, L. (2011). Secrecy throughput of MANETs under passive and active attacks. IEEE transactions on information theory, 57(10), 6692-6702.
15. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. IJ Network Security, 5(3), 338-346.
16. Najafi, G., & Gudakahriz, S. J. (2018). A stable routing protocol based on DSR protocol for mobile Ad Hoc networks. Int. J. Wirel. Microw. Technol.(IJWMT), 8(3), 14-22.
17. Jamal, T., & Butt, S. A. (2019). Malicious node analysis in MANETS. International Journal of Information Technology, 11(4), 859-867.

AUTHORS PROFILE

Shibu K.R, received his Master's degree in Computer Science and Engineering from Manonmaniam Sundarnar University, Tirunelveli and pursuing Phd from Noorul Islam Centre For Higher Education, Nagercoil, TamilNadu. His research interest includes Mobile Ad Hoc Networks and Network Security

Dr. SujiPramila R, is working as an Associate Professor in Department of Computer Science and Engineering of Noorul Islam Centre For Higher Education, TamilNadu ,India. She completed her PhD in computer science and Engineering from Noorul Islam Centre For Higher Education Nagercoil. Her main research interest includes Mobile Communication and Sensor Networks.