ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter11852020.pdf
https://doi.org/10.30534/ijeter/2020/11852020

# A Novel Secret Key Generation Scheme for MANETs using Traffic Load to Avoid Active Attackers

**Shibu K.R[1], Suji Pramila R[2]**
[1] Research Scholar, Department of CSE, Noorul Islam Centre for Higher Education, India shibukarakkattu@gmail.com
[2]Associate Professor, Department of CSE, Noorul Islam Centre for Higher Education, India,sujisymon@gmail.com

**ABSTRACT**

Symmetric key encryption techniques are the base of providing security in Mobile ad-hoc network (MANET) communication. The performance of existing schemes is not providing complete security in many respects. Their level of security may vary depending on several factors like network topology, routing mechanism, presence of malicious nodes, etc. A novel key generation scheme for MANETs deploying one of the truly dynamic system parameters – traffic volume is proposed in this scheme. The efficiency and performance of the technique is analyzed for routing protocol build on reactive methods. The system proposed here is simulated with two different routing environments: DSR and AODV. These two are similar in their on-demand nature of routing but differ in many ways. The complexity of the secret key generation procedure, the packet loss with and without malicious nodes, and detection probability of active intruders are the parameters evaluated through simulation. The analysis proves the applicability and efficiency of the technique to the reactive routing based networks. Also the typical characteristics like node mobility are not affecting the key generation.

**Keywords:** MANETs, DSR, AODV, Traffic load, Key Generation

## 1. INTRODUCTION

The dynamic groups of mobile nodes that are infrastructure-less, without any control stations or routing devices are called MANETs. They are deployed for specific applications where all the nodes need equal priority to become a transmitter or a receiver, like in military rescue operations, disaster management, etc. The typical attributes of MANETs cause them sensitive to adversary attacks. Majority of the attacks in the network is passive and is very difficult to avoid them. This increases the demand for developing secure data communication techniques for them. The current systems are depending on various cryptographic methods to secure data [1]. But the generation of a truly random secret key for cryptography is the real challenge before the researchers.

The generated keys are not unique and universal, so their applicability for different network topology and discrete routing schemes pose a problem in designing key generation algorithms. Another requirement in the generation of a cryptographic key is the 'random source' [2] of data which is the input for the key extraction process.

The routing protocols used by the networks are of three types – proactive, reactive and hybrid. The reactive type routing which is also called as on-demand source initiated routing utilizes some data tables for recording the events occurring at the time of routing. These table entries are later used for finding new routes. As MANETs are highly dynamic in nature, the data recorded in these tables are also dynamic in nature. So these random data entries are employed for extracting the random source for key generation. The survey of many existing works [3] shows that the randomness of the generated key can be increased by exploiting some correlated data variables. This is achieved in the proposed scheme by creating an additional data table that records the traffic of data in the network at each node. The data are stored as a two-dimensional matrix at each node. The system exploits this dynamic attribute of many system metadata for using them as 'random source' for key generation. This work is utilizing the correlated data extracted from both routing and traffic data tables. This technique suits for MANETs operating with reactive routing [4].

The proposed scheme is simulated with NS2 for two most accepted on-demand source initiated routing techniques AODV and DSR [5]. The simulation results are studied to verify the suitability of the scheme for reactive routing based MANETs. The remaining paper is dissected into four sections. The section 2 is a review of the existing works and section 3 presents the outline of AODV and DSR routing techniques. The section 4 describes the creation procedure of traffic matrix and random bit generation. The section 5 outlines the results of simulation and their analysis. Finally, the conclusion is briefed in section 6.

## 2. WORKS RELATED TO KEY GENERATION

The main challenge of the MANET is to ensure protection from intruders. Their very nature is making them vulnerable to several external and internal attacks. The conventional algorithms deployed for routing does not provide any kind of protection to the network. So, these networks are depending on one or more data security measures like key distribution schemes or random bit generators. The schemes for data authentication and security are associated with the routing technique. Authentication of the nodes involved is done using some asymmetric cryptographic technique and validation of messages uses one of the symmetric cryptographic techniques. The adversaries attack by denial of service, eavesdropping, false routing, or any other activity which prevents the message to reach the destination directly.

The survey on proactive and reactive protocols [6] concludes that the reactive ones outperform with the increase in network size. The simulation studies are performed on ad-hoc networks, with different key generation algorithms utilizing these routing protocols.

Usman et [7] al implemented a data securing method for highly dynamic networks. Handshaking signals are used in the analyzed network for communication. The concept uses symmetric encryption for achieving data security. The encryption cost is so high that the storage requirement increases exponentially with the increase in the nodes in the network.

N Alangudi [8] suggested a strengthened key generation method for VANETs, by modifying DH and ECC algorithms. This work mainly focuses on holding up the delay in communication and overhead for the routing. This scheme uses a dual authentication approach to decrease the key generation time and to make the key more secure than existing ones. The main shortcoming of this proposal is delay occurred in key updating. In [9] they have given an in-depth survey on the types of attacks that may happen in MANETs. They have categorized the types of passive and active attacks with examples. Also the various IDS based approaches to solve some among them are mentioned in this review. The survey mentioned that a single Intrusion detection scheme cannot protect the networks from all these types of security

## 3. CHARACTERISTICS OF ON-DEMAND ROUTING PROTOCOLS

The routing protocols applicable to MANETs are either proactive, reactive, or hybrid type [10]. The most accepted ones based on the overhead and bandwidths are reactive protocol strategies. DSR and AODV are two reactive routing techniques. Both these protocols initiate the routing process when there arises a communication demand by broadcasting the route request (RREQ) packet to the neighboring devices present in the coverage area of the transmitting node. The nodes receiving this message respond either by sending a route reply packet (RREP) if the required route to the destination is available in its route cache, or forward the RREQ packet to its nearby nodes. The process continues until the packet reaches one of the nodes having a route record to the destination node or the target node itself. The routes reply message traverses back to the source node. During this reverse traverse of the RREP packet through the intermediate nodes the route record in the packet is copied to the route cache of these nodes. In this way once identified routes are kept as a record and can be used further.

The selected protocols DSR and AODV do the routing in this manner and maintain the routing information each time a new route is discovered. But there exists some difference also. The features in common [11] and the major differences are listed in the Table 1.

**Table 1:** AODV and DSR comparison

| 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 routing tables differ in the two routing protocols, in DSR the entire route is recorded but in AODV the next-hop data is recorded. So in AODV to make it adaptable to the proposed key generation scheme the full rote table is created additionally.

## 4. SECRET KEY GENERATION

MANETs are deployed in applications that require the highest possible security and maximum confidentiality. The very nature of MANETs causes them security issues of both passive and active types. These are prevented or corrected using some of the existing intrusion detection mechanisms.

The common approaches are to encrypt the data with a random binary sequence generated using random number generators or secret key generation algorithms. The survey of these techniques reveals the limitations of these techniques. The computational overhead, complex random source extraction process, the lower entropy level data leaked to the adversary during information reconciliation, etc are some of the drawbacks of the existing schemes. The proposed scheme can overcome the above-mentioned limitations of the present day algorithms by utilizing easily available correlated system metadata the full route data and traffic volume.

### 4.1 Route Table creation

The route table associated with the reactive routing DSR and AODV is the source of information to maintain a full route table. The full route table records four entries: source node ID, destination node ID, RREQ ID, and the list of full nodes included in that route. The route tables at each node are revised whenever a new route is identified in which the node is an intermediary. The tuples of the route table content of any node is shown in Figure 1

| ROUTE TABLE | | |
|---|---|---|
| **SOURCE IP** | **DESTINATION IP** | **FULL ROUTE (FRT)** |

**Figure 1:** Route table entries

### 4.2 Traffic Matrix

The traffic volume is the entire number of information packets moving from a sender node to a receiver node. This data packet movement count can be recorded in the form of a two-dimensional traffic matrix. If the present node name is 'P' and the total number of nodes in the network considered are 'N' then, the traffic matrix can be created as an 'N x N' symmetric matrix. Each entry of the matrix represents the total amount of message packets traversed through the node 'P' for the selected source to destination. The entries of the matrix are shown in Figure 2.

| TRAFFIC LOAD MATRIX | | |
|---|---|---|
| **SOURCE IP** | **DESTINATION IP** | **TRAFFIC LOAD** |

**Figure 2:** Entries of traffic matrix

In the matrix the row and column values are the source ID ($S_i$) and the destination ID ($D_j$) respectively. The matrix entries are the traffic load of individual routes directed from a particular source to destination. If '$S_i$' is the source node and '$D_j$' is the destination node then, traffic load '$L_{ij}$' is the number of packets moved from this source-destination pair through 'P'. The entries of a traffic matrix are shown in Figure 3.

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

**Figure 3:** Traffic load matrix

The traffic load entry for a node can be obtained as the cumulative sum of all the data transfer between any two source-destination pairs in the network. This can be expressed as a mathematical function as given below;

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

Where, 'Rp' is the list of entire route for a source-destination pair through node 'P' and N(S, D; Rp) is the data volume through that routes.

The matrix entries are getting updated along with the updating of the routing information after each route identification process. Since all the nodes in the network have equal probability to become source and destination at any time, these processes are truly random. So the route records and traffic matrix values are dynamic enough to ensure the needed randomness for utilizing them as random sources.

### 4.3 Extraction of random source.

The secret key generation process is accomplished at the two communicating nodes with a set of random source data which are alike at the two nodes. The random source for the key generation must be random. In the proposed scheme the route table entries and traffic matrix data are used to extract a correlated set of random variables that can be used as a source for key generation.

Consider that the two communicating nodes are 'P' and 'Q'. These nodes perform a set of identical secret source data extraction steps. The algorithm for this is given below;

**Step1:** let the node 'P' be the source and node 'Q' be the destination.

**Step2:** Source node sends a message to a destination asking the willingness for communication and checks whether the response is positive. If it's positive then goes to step 3else resend the message till it gets a positive response.

**Step 3:** The source node 'P' creates a list of routes that include both these nodes. The first list of the source-destination (SD) pairs.

$$SDL1 [\ ] = Si - Dj(P, Q) \epsilon FRT(P)$$

**Step 4:** Now create a second list of SD pair list from the first list in which only 'P' is appearing as an intermediary.

$$SDL2 [\ ] = \{Si- Dj (P) \in SDL1[\ ] \} \&\&$$

$$\{Si - Dj (P) \in FRT(P) \}$$

**Step 4:** Extract the final list by removing the second from first

$$SDL [\ ] = SDL1 [\ ] - SDL2 [\ ]$$

**Step 5:** The extracted SD pair list is used to get the traffic load values from traffic matrix for these SD pairs;

$$SBTL [\ ] = \text{for all } SDL [\ ]\{ L_{ij} \in TLM(P)\}$$

**Step 6:** The sub- matrix obtained SBTL [ ] can be used as 'random source'.

**Step 7:** All the entries of this sub-matrix is assigned with a binary string. These binary numbers are ten XORed to get the random bits.

At node 'Q' these steps are executed to get the same set of random bits. The random bit length can be decided by the network depending on the security level needed. The length of random bits and the security are directly proportional that the security and randomness increase as the number of bits increases.

## 5. RESULT ANALYSIS

The key generation scheme using traffic metadata is simulated here. The tool used for simulation is NS-2. The various metrics used in the simulation environment are shown in Table 2. The simulation is carried out in two scenarios; one is a network that uses DSR and the other is AODV. Both of these schemes have their advantages and disadvantages. For the analysis purpose, the parameters considered here are delay in key generation procedure, time for computation, packet loss, and the detection of active attackers.

**Table 2:** Metrics used 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 |

### 5.1 Delay incurred in key set up

As we discussed earlier, both of the routing schemes will be having some dissimilarities in the method of storing the full route information used for route identification, all though they are using the same flooding technique for routing. The AODV protocol stores only the next hop data while the DSR records the entire route information at all the individual nodes after the route recognition. For this, our approach DSR will be more suitable which will be proved in the following sections. In AODV additional storage is required for the retaining and recording of the route details. By utilizing the details such as hops that are already in the system reduced the overhead further. The time for the randomness extraction can be calculated by summing up the source-destination duo from the table FRT (p) and the total time required for the extraction of traffic data values which are available in the matrix TLM (p).

$T_{avg}$ = *f (Extraction time for list of SD pairs + Extraction of corresponding traffic load* )

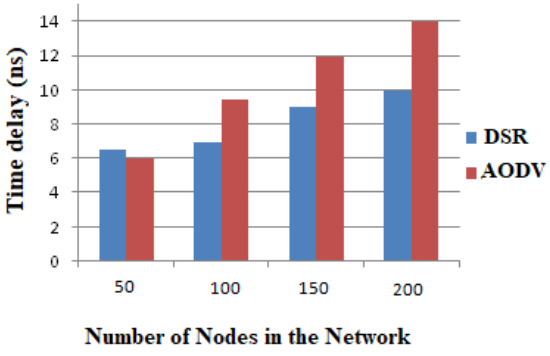


**Figure 4:** Node number Vs Delay time

The simulation results in Figure 4 prove that time delay incurred is less when the number of hosts in the network is low. So the AODV based scheme will be applicable for networks with a lesser number of nodes.DSR based approach will suits bigger networks with less time and computational complexity.

### 5.2 Ratio of Packet delivery

PDR is the most common metric used for the evaluation of network performance. It is the correlation between the total packet arrived at the target node and the count of packets which are delivered from the source. This ratio is contingent on numerous agents such as strategy for routing, re-routing, link breakage, node mobility, the existence of malicious nodes [12], etc. Although both AODV and DSR are not table-driven, their judicious approach for steering the erroneous paths is distinct [13]. Fundamentally, DSR is the most efficient scheme to redirect the messages through other routes which are existing to the given destination in the case of link break. Both of the protocols lack congenital security mechanism or safeguarding techniques.

The imitation was carried out by presuming that the mobility of the host in the network is less, to make sure that the link breakage and rerouting is as less as possible. The productivity of the key generated is trying out by ranging the adversary nodes in the simulated network. Simulation was carried out for both the key generation schemes i.e. based on the traffic load and the normal randomness generation. The result of this approach is shown in Figure 5.

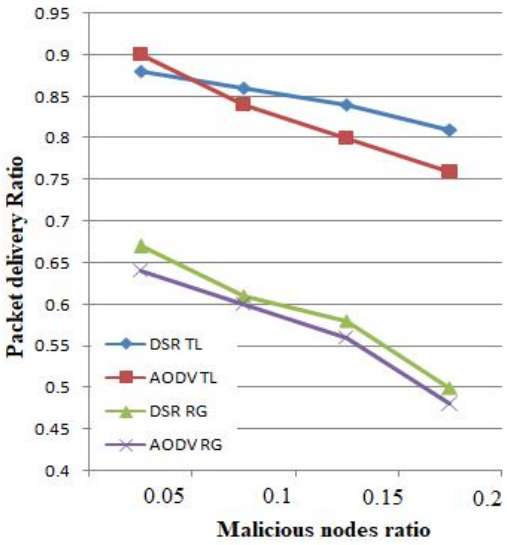


**Figure 5:** Effect of adversaries on packet dropping

As we anticipated the PDR was very high for the key generation using traffic metrics. The noticeable factor is the PDR is practically continual for the DSR environment. While for AODV, the ratio will be reduced with the growth in the number of eavesdropping nodes

### 5.3 Observation of Active attacker

The attackers are broadly categorized into two 1) active attackers, those nodes which will actively participate in the transmission of messages by forwarding the modified content. 2) Passive attackers who do not try to be part of the communication, but will listen to the information that is propagated in the given network. The majority of the current techniques focus on the identification or elimination of the passive attack by some key generation schemes. As we mention in the earlier section, that the proposed scheme will create and update traffic based matrix for draw out the random sequences, to generate the secret key to protect the network from active attackers. Make use of the traffic metadata for the identification of active attackers is the major highlight in this scheme. The latest works [14-16] exhibits that the active attack in the network will try to tail the information involved in the communication. In [17] it is proved that the active attacker will set off the major paths to take apart in the packet transmission.

The TML(p) is the matrix which holds the traffic details of node 'p' will be updated whenever a packet is if forwarded through this between any pair of nodes in the networks. If a node says '$N_1$' is doubted as an active attacker, then it can be identified here in two steps 1) Probe in its full route catalog for the existence of a node '$N_1$' as an intermediate node in more than 70% of the full route entries 2) Calculate the average of all the entries in traffic load '$L_{est}$' in which node '$N_1$' is an intermediate node. If the value is greater than the pre defined minimum value then the node 'N1' will be probable active attacker.

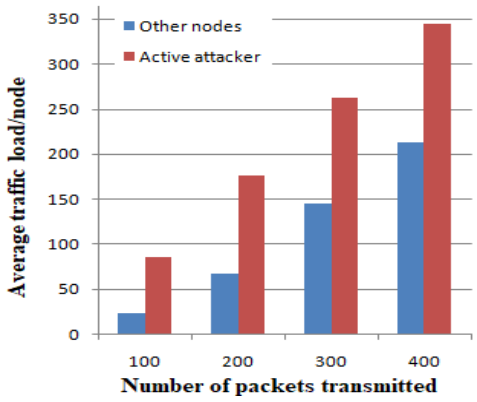


**Figure 6:** Traffic load Vs Packets transmitted

The figure 6 reveals that the node which behaves as an active attacker will try to enter in all the active routes nearly along with a considerable increase in the average load value for the concurred attack node

## 6. CONCLUSION

As the security of MANETs is a major concern, here a novel key generation technique is implemented with two different routing approaches. This key generation scheme mainly suits for the network which uses On Demanding protocol for the routing process. The performance of DSR is better when compared to AODV in various scenarios such as the speed of key generation, loss in packet delivery, storage, and computational overhead. The result of the simulation is compared with an existing scheme and it shows that this scheme will suit for networks where the number of the active attacker is high. Thus the key generation using the traffic metadata can be applied in various other routing protocols. Due to the significance of security in MANET, this method is more suitable as the computational overhead is less.

## REFERENCES


1 Sarangapani, J. (2017). ***Wireless ad hoc and sensor networks: protocols, performance, and control.*** CRC Press. https://doi.org/10.1201/9781420015317

2 Shibu, K. R., & Pramila, R. S. (2019**). Random Bit Extraction for Secret Key Generation in MANETs.** *Wireless Personal Communications*, 1-15. https://doi.org/10.1007/s11277-019-06381-3

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. https://doi.org/10.1109/IWCMC.2018.8450367

5 P. Srikanth Reddy, P. Saleem Akram, M. Adarsh Sharma, P. Aditya Sai Ram, R. Pruthvi Raj (2019) **Study and Analysis of Routing Protocols,** International Journal Of Emerging Trends In Engineering Research.7(11),434-440. https://doi.org/10.30534/ijeter/2019/067112019

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 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 R.Srilakshmi & Jayabhaskar(2020**). Elliptic curve cryptography based security protocol of manet under dynamic cluster head selection environments.** International Journal Of Emerging Trends In Engineering Research.8(2),447-454. https://doi.org/10.30534/ijeter/2020/32822020

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. https://doi.org/10.1007/s41870-018-0168-2