KEY DISTRIBUTION APPROACH TO MITIGATE PASSIVE ATTACKS IN MANET

Usha M S
Research Scholar, Dept. of CSE,VTU-RRC, VTU, Belagavi,
Associate Professor, Department of CSE,NIE Institute of Technology, Mysuru, Karnataka, India
msusha.2010@gmail.com

Dr. K C Ravishankar
Department of Computer Science & Engineering, Govt. Engineering College, Hassan, Karnataka, India
Visvesvaraya Technological University, Belagavi, India
kcrshankar@gmail.com

Abstract - Dynamic nature of the MANET has wide variety of opportunities for the innovative researchers to think and propose varied solutions to upgrade the communication system. Because of the dynamic nature of the environment, security measures play a major role. The same nature is considered as strength of the environment in this paper. Resolutions of the Passive attacks in the MANET AODV routing is one of the challenging requirement corresponding to security aspect of the environment. In this regard, the proposed paper is trying to introduce a revolutionary key distribution algorithm by adding few columns into existing AODV routing table. Also the paper is verifying the performances of the regular AODV and the proposed algorithmic framework corresponding to end-to-end delay, throughput and packet drop parameters of the network. Network Simulator 2 is employed for the parameter estimation of the proposed and existing systems.

***Keywords*:** MANET; AODV routing; Passive attacks; NS2 simulator.

1. Introduction

Mobile Ad-hoc Network (MANET) is a communication environment connecting non-stationary devices through one of the routing algorithms namely AODV, DSR, ZRP, DSDV and so on. Non-stationary devices or components create a dynamic topological structure by allowing new nodes in the communication environment [1]. This property of the MANET may create unsecured and vulnerable environment. Malicious nodes not only disturb (dynamic or active attacks) the communication environment also allows eaves droppers (detached or passive attacks) to leak secured information. There are several proposals [2] addressed the active attacks by introducing number of algorithms, frameworks and so on. But, several studies [3] say's passive attacks are more challenging to address in the environment. Hence, this paper is trying to attempt an algorithmic framework to deal with passive attacks through key distribution techniques.

Encryption and decryption are the techniques used to secure the data from the eaves droppers in the communication environment [4]. Encryption generates a cypher data from a normal data then forward the same towards receiver. Receiver applies Decryption process on received data to convert cypher data to normal data for its further usage.

The dynamic nature of the MANET would become a positive parameter for resolving passive attacks. This paper is trying to split the key into two parts and route them through different paths to reach destination. A simple RSA is employed to perform encryption and decryption activities at sender and receiver side respectively.

2. Literature Survey

This section introduces some of the existing proposals, algorithms and solutions exists from the literature.

2.1. *MANET and its routing protocols*

Mobile Ad-hoc Network is a self-designing network relying on framework, likewise is a huge innovation which supplies virtual equipment and programming assets according to prerequisite of MANET [5]. Due to its dynamic topological structure creates several challenges or opportunities routing, security, energy efficiency and performance for the researchers. The author [6] proposed four procedures to defeat the energy efficiency issues in past investigations of content routing of NDN based MANET, they are Decreasing flooding and flooding traffic exercises, Diminishing reliance on remote transmission moves toward just for certain conditions, The utilization of bio-inspired way to deal with make content more versatile and efficient routing and better

utilization of information structure and Information configurations to spare energy, storage area, and network transfer speed.

Routing in MANET is demanding because of development of nodes. Anticipating the nodes position and routing dependent on anticipated positions assists with building up routing way with much life span. Most expectations approaches depend on the past areas of the node. A multi way routing protocol dependent on assessed likelihood areas with way routing at fundamental spots along way is proposed for improved routing execution without bigger packet overhead [7]. The secrecy throughput of MANETs with pernicious nodes is examined. The MANET comprises of authentic versatile nodes and pernicious nodes. Transmission between real nodes are dependent upon a postpone limitation [8].

2.2. *Passive attacks*

Author [9] has listed a few assaults as indicated by various layers in Ad-hoc network, their conduct, source, included nodes and disregarded security administrations. Also he claims that, as specially appointed networks are defenseless against numerous sorts of assaults, the assurance of such networks is a difficult issue. Network coding is a reformist data spread innovation for network interchanges. Here author has presented an extensive audit of the investigation on secure network coding against passive assault [10]. Author [11] has proposed a framework comprises of three principle blocks: they are assault classification, fuzzy implementation and fuzzy estimation [12]. These blocks are utilized to categorize the type of assault or attack in the MANET environment.

2.3. *RSA Encryption technique*

Cryptographic procedure is one of the chief ways to ensure data security. Not just has it to guarantee the data private, yet additionally gives signature, confirmation, secret sub-stockpiling, framework security and different capacities. Along these lines, the encryption and decoding solution can guarantee the privacy of the data, just as the integrity of data and certainty, to keep data from altering, falsification and duplicating. Author [13] explored RSA public key and other related innovation applications in the military, business, protection and different fields of data security which assumes a significant job. RSA is a solid encryption algorithm that has stood an incomplete trial of time [14]. The normal size of n must increment with time as more efficient calculating algorithms are made and as PCs are getting quicker.

Author [15] creates three tests so as to look at the execution season of the cycles of encryption and decryption and comparing the outcomes along with evoke the improved focuses and talking about them. In addition, some programming strategies were utilized so as to accelerate the cycle of encryption or decryption. The outcomes show that the execution season of encryption measure was improved by 14% in test 3 by utilizing a few procedures to accelerate the cycle; the decryption cycle was improved also by 22%. Based on outcomes author affirm that the quality of calculation utilized in framework is the RSA algorithm, which is one of the most remarkable encryption calculations. Despite the fact that RSA is the most utilized encryption algorithm today, it has a few impediments to consider with the end goal for RSA to remain the best and exploration ought to be done to make quantitative RSA opposition.

3. The proposed key distribution approach

Figure 1 demonstrates the possibility of passive attacks in AODV routing protocol of MANET. Node A has found the route A→ G → H → D. Here an assumption is made that the Node G is passive attacker. This is one of the major threats in the vulnerable environment as per the existing AODV routing protocol. Detection of the passive attacks in the environment is one of the major challenge because of its hidden participation during communication.

Key distribution approach introduces Split, Combine and Secure (SCS) algorithm to mitigate malicious passive attacks. RSA algorithm is employed at the network layer of the MANET for encryption and decryption process of the data packets. Figure 2 demonstrate the different parts of 1024 bits RSA key of 512 bits each. Figure 3 shows the Ad-hoc communication between source and destination nodes A and D. Since, data packet is encrypted and transmitting along the path from source A through destination D, number of malicious passive attacker nodes may exist. Because of the encrypted data packet and unavailability of the complete key, none of the passive attacker can decrypt the data packet. Two different parts of the key, key-part1 and key-part2 are transmitted at different routes.

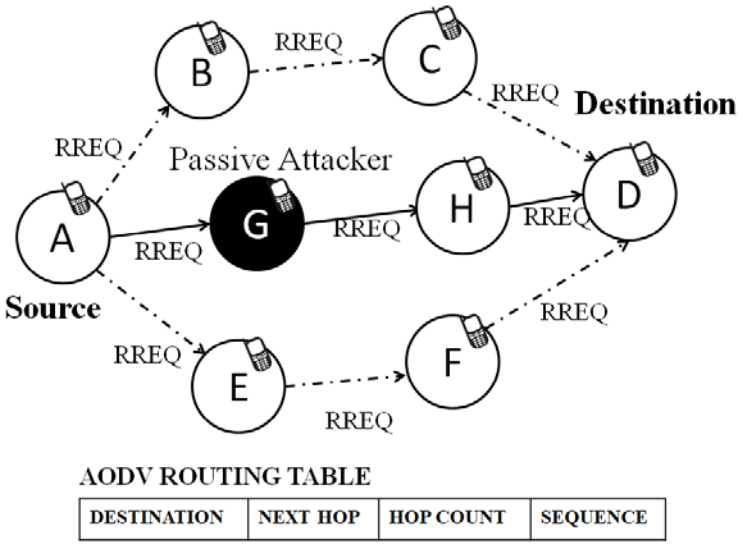


Fig. 1. Example scenario for Passive Attack

Algorithm 1: Split, Combine and Secure (SCS)

Step1: Generate key using RSA encryption

Step2: **Split** key into two parts

Step3: Choose two different routes using AODV protocol

Step4: Send parts to the key

Step5: Receive and **combine** the parts of the key

Step6: Perform RSA Decryption

Step7: Receive **secured** data

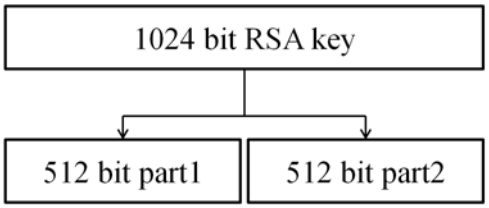
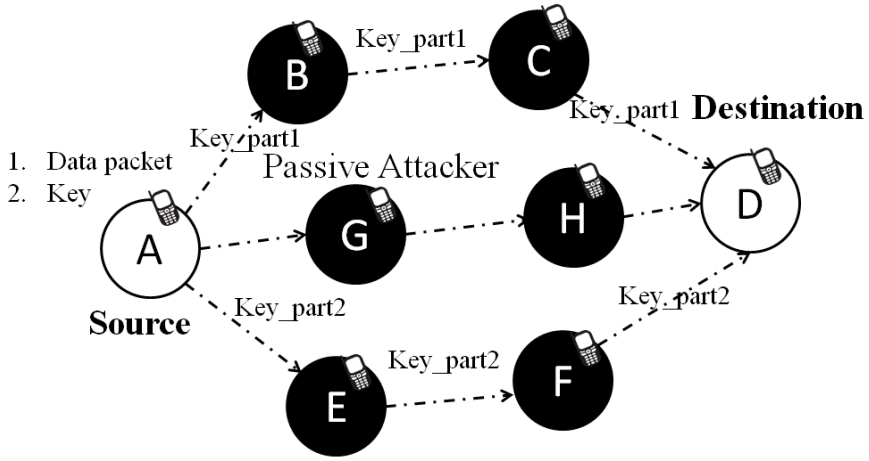


Fig. 2. Two parts of 1024 bit RSA key

To differentiate between key and a data packet, another column is added in the existing AODV routing table as shown in Figure 3. Also, it is depicting the secured environment in Ad-hoc communication even though there exists any number of passive attacker nodes.

4. Results and Discussions

Network Simulator NS 2 is used to implement and verify the performance of the proposed framework with the existing regular AODV routing. Simulation is conducted with the network configuration as shown in Table 1.



AODV ROUTING TABLE

DESTINATION	NEXT HOP	HOP COUNT	SEQUENCE	KEY

Fig. 3. Proposed framework Example scenario for Passive Attack

Table 1. Simulation configuration in NS2

Parameter	Values
Channel type	Channel/Wireless Channel
Radio-propagation model	Propagation/ TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue
Link layer type	LL
Antennae model	Antennae/Omni Antennae
Number of nodes	6
Simulation time	38s
Routing protocol	AODV
Maximum speed	2m/s – 20m/s
Transmission range	250 meters
Simulation area	900 * 900 meters
Packet size	1000 bytes
Queue size	50
Number of channel	2-3

Figure 4 shows the regular AODV routing and its communication from source to destination by assuming path. Similarly Figure 3 demonstrates the proposed framework. Here the data packets, key-part1 and key-part2 transmissions are routed in three different paths simultaneously. Throughput, end-to-end delay and packet drop parameters of the data transmission are estimated in both the cases and recorded them in Table 2.

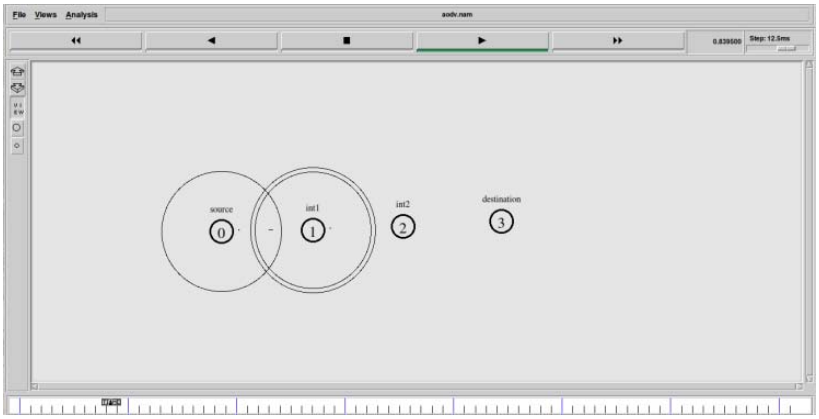


Fig. 4. Regular AODV communication

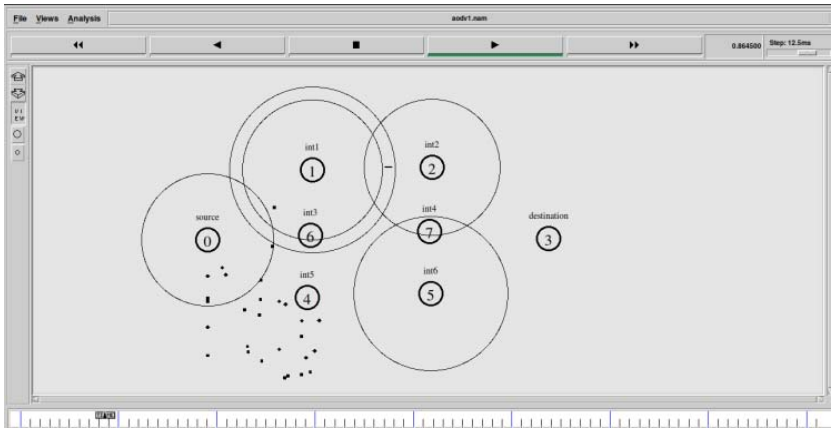


Fig. 5. Proposed key distribution based AODV communication

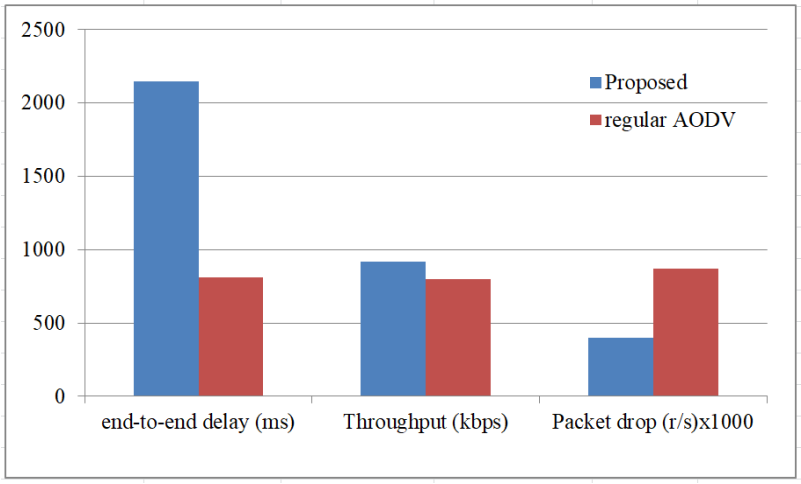


Fig. 6. Performance comparison with regular AODV with Passive attacks

Table 2. Estimation of network parameters during simulation

	End-to-end delay(ms)	Throughput (kbps)	Packet drop (r/s) x1000
Proposed	2146.18	920	397.7
Regular AODV	813.38	795.93	867.8

Figure 6 is the plotted graph corresponding to the estimations recorded in Table 2. Graph is clearly depicting that the proposed framework to ensure the security of the data from the eaves droppers is time consuming. It is due to the additional key transmission at different paths. Because of the multiple paths for the data transmission, the packet drop in the data transmission is reduced thereby increases the overall throughput environment.

5. Conclusion

An attempt has been made to propose a key distribution approach to mitigate malicious passive attacks in MANET. Performance of the communication network plays an important role during data transmission and at the same time secured communication also important parameter to ensure. This paper concludes that, the proposed framework may not be good with respect to time parameter but it ensures utmost security of the data during transmission. The additional aspects may burden the communication but guarantees the security of the data. Hence, the proposed framework can be used in the applications where security of the data has been given first priority.

Acknowledgments

I would like to express my deep and sincere gratitude to my Research Supervisor Dr. K C Ravishankar, Professor and Head, Department of Computer Science and Engineering, GEC, Hassan for giving me the opportunity to do research and providing me incredible guidance throughout the research. I am deeply indebted and extremely thankful to our NIEIT Management and Dr.Bansilal, Principal for their continuous support extended throughout my research work. I express my heartfelt thanks to my loveable family members for their constant support.

References

[1] Maan, Fahim, and Nauman Mazhar. "MANET routing protocols vs mobility models: A performance evaluation." 2011 Third International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2011.

[2] Tayal, Supriya, and Vinti Gupta. "A survey of attacks on manet routing protocols." International Journal of Innovative Research in Science, Engineering and Technology 2.6 (2013): 2280-2285.

[3] Liang, Yingbin, H. Vincent Poor, and Lei Ying. "Secrecy throughput of MANETs under passive and active attacks." IEEE transactions on information theory 57.10 (2011): 6692-6702.

[4] Goshwe, Nentawe Y. "Data encryption and decryption using RSA algorithm in a network environment." International Journal of Computer Science and Network Security (IJCSNS) 13.7 (2013): 9.

[5] Vinayagam, Jaikumar, C. H. Balaswamy, and K. Soundararajan. "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection." Procedia Computer Science 165 (2019): 196-208.

[6] Farkhana, Muchtar, et al. "Energy conservation of content routing through wireless broadcast control in NDN based MANET: A review." Journal of Network and Computer Applications 131 (2019): 109-132.

[7] Farheen, NS Saba, and Anuj Jain. "Improved routing in MANET with optimized multi path routing fine tuned with hybrid modeling." Journal of King Saud University-Computer and Information Sciences (2020).

[8] Liang, Yingbin, H. Vincent Poor, and Lei Ying. "Secrecy throughput of MANETs under passive and active attacks." IEEE transactions on information theory 57.10 (2011): 6692-6702.

[9] Meddeb, Rahma, et al. "A survey of attacks in mobile ad hoc networks." 2017 International Conference on Engineering & MIS (ICEMIS). IEEE, 2017.

[10] Liu, Yantao, and Yasser Morgan. "Security against passive attacks on network coding system–A survey." Computer Networks 138 (2018): 57-76. [8]

[11] Balan, E. Vishnu, et al. "Fuzzy based intrusion detection systems in MANET." Procedia Computer Science 50 (2015): 109-114. [9]

[12] Amiri, Ehsan, et al. "Intrusion detection systems in MANET: a review." Procedia-Social and Behavioral Sciences 129 (2014): 453-459.

[13] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th international forum on strategic technology. Vol. 2. IEEE, 2011. [11]

[14] Milanov, Evgeny. "The RSA algorithm." RSA Laboratories (2009): 1-11. [12]

[15] Al-Kadei, Faten H. Mohammed Sediq, Huda Abdalkaream Mardan, and Nevart A. Minas. "Speed Up Image Encryption by Using RSA Algorithm." 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2020.