International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Reliable AODV for DANET using Homomorphic Encryption Scheme

Manoj Kumar G, M. Abdul Rahiman

Abstract*: DANETs, when compared to MANETs, have high network density and mobility over time. To maintain a secure communication over DANET, requires the knowledge of mobility and complex key management scheme based on the topology change. Operation of DANETs can be categorized into two types based on the activity: 1. Activities requiring small key length 2. Activities requiring large key length. For disaster detection and emergency rescues, key length with reduced size (partial authentication mechanism) is preferable, whereas military operation or critical data sharing needs larger key size (complete authentication mechanism). The challenges for key management in DANETs include the identification of which routing information to be trusted, legitimate nodes with the key for conducting safety communication. Maintaining existing key management schemes over network density change leads to a complex routing and data handling methods.. In this paper we propose a novel approach of homomorphic encryption scheme for data communication security by combining network protocol steganographic security management scheme which reduces the critical information leakage in DANETs. The proposed algorithm helps to identify the distributed denial of service attack and identification of malicious nodes. The malicious activities in a group are identified by analysis of link failures, retransmission information encoded over application layers. In order to assure reliability, encoded data is used as a means to monitor, detect and remove malicious nodes from routing table. We conduct simulation experiments by using network simulator 3.26, Open street Map to verify that our method achieves significant improvement in preventing critical data leakage in presence of malicious nodes.

Keywords: DANET, Homomorphic Encryption, malicious node.

I. INTRODUCTION

Now a days any virtual or physical device having mobility connected to some sort of network can be considered as a part of MANET. The exponential growth of connected devices will reach to 21 billion according to Gartner [1] by 2020. Like MANETs, DANETs are infrastructure less networks with high density of mobility. As more and more devices are connected to the Internet risk of being attacked also grows exponentially. MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Hence routing protocols must encapsulate an essential set of security mechanism against the active and passive attacks. Attacks in DANET can be classified as the following types: intrusion detection – a) centralized b) distributed denial of service, black hole, worm hole, counterfeit routing information etc. Trust based security schemes use extensive security solutions to avoid false positives and to detect the packet loss in a proactive demeanor. Undetectable malicious nodes help to decrease the security, performance degradation and subsequent degradation/disconnection of network. Due to the lack of a trusted centralized authority and limited resources, DANETs are more susceptible to security attacks. In this paper we propose a hop based fully homomorphic encryption method along with a network protocol steganographic method to check the integrity and security of packets transmitted using AODV protocol.

II. PROBLEM STATEMENT

For maintaining communication security among managed nodes in DANETs dynamic secure addressing schemes have been introduced using IPv6. Pure or open DANETs do not have any exchange of pre-determined security parameters like public key, certificates etc. for connection establishment [2]. The objectives of a standard protocol for addressing DANETs include uniqueness (flawless routing), robustness (desist address conflict), scalability (steady state of transmission even after the induction of new nodes), reliability (deliver confidential information over a network having any type of attack). To further enhance the reliability of AODV protocolwe introduced homomorphic encryption method among ‘n’ nodes in a DANET. To ensure reliability against various attacks and data leakage, hop based network protocol encrypted identifiers was applied in application layer.

III. RELATED WORK

The existing secure communication methods use preconfigured nodes on managed nodes that have prefixed public keys, certificates, session parameters etc. The buddy system technique used by Cavalli and Orset [2] maintains a block of available addresses in the network. The block of available addresses is divided into two equal parts. One-half of the available address is given to the requester nodes and the remaining half will be kept with the initiator node for future use. It is difficult to manage address blocks for the individual nodes in a MANET.

Manuscript published on November 30, 2019.
* Correspondence Author
Manoj Kumar G*, Research Scholar, Department of CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
M Abdul Rahiman, Research Guide, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.

To overcome the management of address block, Virtual address space mapping (VASM) [3] was proposed by Taghiloo et. al. Here requester sends a one-hop broadcast message to find an initiator. An initiator obtains a new address from its Allocator node and assigns it to the Requester. Another lightweight secure address configuration scheme uses VASM addressing technique for address allocation along with secret key and symmetric cryptographic function to avoid security threats. Even though these nodes are secure enough they are prone to attacks that mitigate unwanted information among various channels. Security with undetectable characteristics evolved as steganographic methods in protocols. The network steganographic methods are divided into four categories: storage, timing, hybrid and transform methods. Packet reordering, one of the earlier method for network steganography used different sequencing of multiple packets to build a covert channel. For 'n' packets, n! permutations are used to encode secret information, thus a maximum of $\log_2(n!)$ bits can be covertly transferred. Another kind of covert channel based on packet ordering [5] by Atawy and Al-Shaer, used out-of-order packets to represent information. It does not depend on packet payload and is not sensitive to inter-packet delay jitter. The number of different queues represents the steganography bandwidth. Using this method, for 'n' packets, the steganography bandwidth is between $\log_2(n!) \sim n\log_2 n$. The above mentioned steganographic methods use intra-protocol steganographic methods. In order to improve the weakness of the intra-protocol steganography,

Inter-Protocol Steganography (IPS) method was introduced. The IPS method by Jankowski et al. [6], used the relationships between two or more different protocols to build covert channels. These different protocols can be in the same layer or different layers of TCP/IP protocol stack.

IV. SYSTEM MODEL

A traffic model was simulated using encrypted node identifiers (RC4 algorithm), hashed message codes, time stamp of messages, mobility information for 10 minutes to study the node mobility behavior and loss/gain in transmission. Data encryption over packets was done using homomorphic encryption for 'n' nodes. Neighbor connectivity is established using HELLO messages. Each node maintains its own copy of neighbor information that are at 1 hop / 2 hop distance. The proposed approach uses the following modified RREQ (Fig-1) and RREP (Fig-2) format. It maintains an additional field called Node Identifier, which carries the encrypted form of the node, traffic information.

Type	Flags	Reserved	Hop count
RREQ (Broadcast) ID			
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			
Node Identifier			

Fig-1: RREQ Message format

Type	Flags	Reserved	Hop count
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			
Node Identifier			

Fig-2: RREP Message format

Consider the scenario of 1/2 hop communication exchange shown in Fig-3.

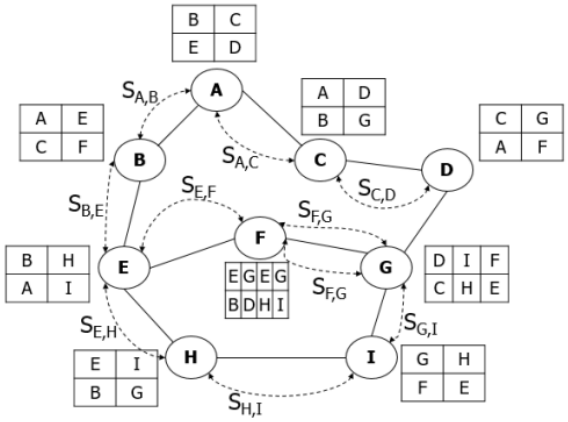

Fig-3: Scenario of 1 / 2 hop communication exchange.

If node A wishes to communicate with node I (assuming key exchange happens using protocol steganography over managed nodes), then Node A sends RREQ to the neighboring nodes that contains the address of the destination. Node A will send an encrypted data using secret key generated from node A for node B or C respectively with time stamped session id, traffic parameters was exchanged.

1. RREQ forwarded to next hop will also follow the same step to its neighbors.
2. When the packet reaches destination, the RREQ which contains the encrypted information is decrypted by the receiver.
3. The destination node in turn follows Step 1 with 1-hop encryption process with its RREP.

The scenario of data transfer can be considered in two different ways:

a) Without DoS attack
b) With DoS attack (black hole, worm hole etc.)

Case 1:

Source node sends data which contains the encrypted message (message id with prefixed time stamps for which the destination node has to wait for forthcoming messages, current location and mobility information). Since the encryption uses RC4 algorithm with 1024-bit key, the time stamped information will be secure enough within the stipulated encrypted period of time.

Case 2:

DoS attack is a type of attack that a malicious node impersonates a destination node by sending forged RREP to a

source node that initiates route discovery, and subsequently divests data traffic from the source node. When a DoS attack is induced into the MANET, a new RREQ with encrypted information for malicious node is the only available information for the neighboring node. RREP Sequence number from malicious node is not sufficient for route selection and change in routing information. It has to reveal the identity as encrypted information, which subsequently has to be recognized and approved by its neighbors. In black hole attacks, the node will consume the packets from the source, here the packet transfer will never happen since the encrypted RREP from destination is not known to the malicious node for the limited time stamped in previous messages. Subsequent to RREP, the destination has to respond for the source node. Since the source node doesn't have acknowledgment/reply fortime stamped operation due to DoS attack, removal of malicious node is made easy.

V. ALGORITHM AND MATHEMATICAL MODEL

Homomorphic encryption allows computation on cipher texts, generating encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. It allows computation on encrypted data. A homomorphism is a transformation from one algebraic structure into another of the same type preserving the structure. Homomorphic secret data sharing is used to transmit a secret data to several recipients as follows:

a) Transform the secret information using homomorphism.
b) Split the transformed secret information into several parts for each recipient.
c) The secret information must be split based on the rule that it can only be recovered when all or most of the parts are combined.
d) Distribute the parts of the secret information to each of the recipients.
e) Combine the recipient's parts to recover the transformed secret information.
f) Abrogate the homomorphism to recover the original secret.

Implementation of Homomorphic Encryption involves functions like encryptor, decryptor, key generator, encryption parameters, coefficient modulus, plaintext modulus, etc.

Table-1 represents the notations used in homomorphic encryption and decryption system

Table – 1 Notations used.

Parameter	Description
q_c	Coefficient modulus in the cipher text space
p_t	Plain text modulus in plain text space
E_{Vk}	There are $E_{Vk}+1 = \lfloor \log_w qc \rfloor + 1$ elements in each component of each evaluation key
w	A base into which cipher text elements are decomposed during relinearization
Δ	Quotient on division of $\frac{q_c}{p_t}$ or $\left\lfloor \frac{q_c}{p_t} \right\rfloor$
$r_t(q_c)$	Remainder on division of $\frac{q_c}{p_t}$

Consider nodes: n_0, n_1… n_k needs to send message M= {m_1, m_2, m_3… m_k}; where message m of n_0 is represented by m_{n0}. Cipher text of node n_0 is represented by C_{n0}.

Therefore, node n0, has message, m_{n0} = {m_{0n0}, m_{1n0}... m_{kn0}}, Cipher text C_{n0} ={c_{0n0}, c_{1n0}...c_{kn0}}.

Overall message encryption of nodes n_1 through n_k is summarized in Fig-4.

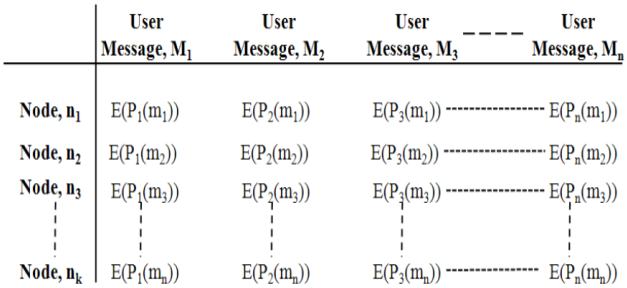

Fig-4: User message encryption over node n_1 through n_k.

Applying additive Homomorphic property over 2-hop node encryption we get,

C'_{add} = ([m_0+n_0]q, ... ,[m_j+n_j]q, ..., [m_k+n_k]q) where

C_1 = (m_0,m_1...m_j), C2= (n_0, n_1... n_k).

Decryption of cipher text is done by computing

$$\left\lfloor \left\lfloor \frac{p_t}{q_c} \left[c(s) \right]_{qc} \right\rfloor \right\rfloor_t = \left\lfloor \left\lfloor \frac{p_t}{q_c} \left[c_0 + c_1 + \ldots + c_k s^k \right]_{qc} \right\rfloor \right\rfloor_t$$

The Node Identifier in RREQ and RREP includes hashed, time stamp value of original message represented as h(M), t_s(M) respectively. Here original message, m is split into blocks of size 64 bits represented = {m_1, m_2, m_3…m_n}. Similarly hashed value of message, M: h(M);

h(M) = { h(m_1), h(m_2), h(m_3),…, h(m_n)}.

Time stamp for M, t_s(M) = {t_s(m1),t_s(m2),t_s(m3)…t_s(m_n)}.

1st hop message, M_1 =E(M_1)$_{\{msg1,n\}}$= {E{$m_{1,1}$||h($m_{1,1}$)||t_s($m_{1,1}$)}}, {E{$m_{1,2}$|| h($m_{1,2}$) || t_s($m_{1,2}$) }}… {E{$m_{1,n}$|| h($m_{1,n}$) || ts($m_{1,n}$)}}

2nd hop message, M2 = E(M2){msg 2,n} = {E{ $m_{2,1}$|| h($m_{2,1}$) || t_s($m_{2,1}$)}}, {E{ $m_{2,2}$||h($m_{2,2}$)||t_s($m_{2,2}$)}} … {E{$m_{2,n}$|| h($m_{2,n}$) || ts($m_{2,n}$)}}

Similarly **n^{th} hopmessage**, M_n = E(M_n){$msg_{n,n}$} = {E{$m_{n,1}$|| h($m_{n,1}$) || t_s($m_{n,1}$)}}, {E{$m_{n,2}$|| h($m_{n,2}$) || t_s($m_{n,2}$)}} …{E{ $m_{n,n}$||h($m_{n,n}$) || t_s($m_{n,n}$)}}

Finally we get

$$\sum_{i=1}^{n} E(Mi)_{(msgi,\,n)} = E(M1)_{(msg1,\,n)} + E(M2)_{(msg2,\,n)} + \ldots + E(M2)_{(msgn,\,n)}$$

for entire node transmission.

VI. SIMULATION RESULTS AND ANALYSIS

Performance evaluation:

The experiments for the performance evaluation of the scheme that validate the detection and isolation efficiency of the proposed scheme against DoS attacks have been carried out using the network simulator ns-3. The simulations consist of 100 nodes evolving in a region of (750m X 750m) during 600 seconds. Transmission range is set to 200 meters. Random waypoint movement model in ns3 is used and maximum movement speed is 15 m/s.

Packets among the nodes are transmitted with constant bit rate (CBR) of one packet per second, and the size of each packet is divided into 16 blocks (1024/64 bytes) due to encryption of data and headers. In the simulation we used two evaluation metrics. Performance comparison is made on the basis of following metrics. Throughput and Packet Delivery Ratio between existing AODV and proposed AODV. Packet Delivery Ratio (PDR), is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This ratio determines the reliability of data packet delivery. Packet loss notifies us about the amount of control packets fails to reach its destination in a timely mode. The percentage of packets dropped increases as both the speed and the number of nodes increases. Link connectivity issues arise if the mobility pattern is not explored and induction of malicious node will also be high. Throughput is the average rate of successful message delivery over a communication channel.

Experimental Results

The OSM file generated from http://www.openstreetmap.org was used for the traffic simulation (shown in Fig-5) and analysis in ns3. Encrypted node data is transmitted with and without DoS attacks. Packet delivery ratio and throughput analyzed is presented in Table-2 and Table-3 respectively.

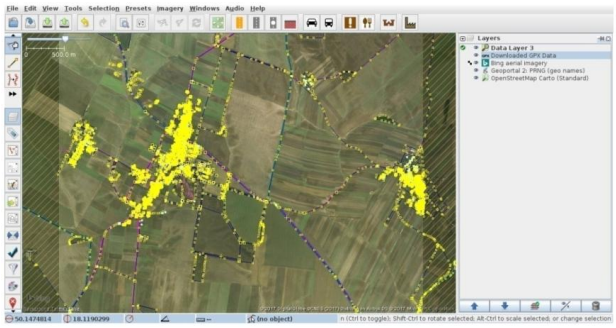

Fig -5: Open street map used for traffic analysis

Table-2: AODV without DoS Attack

Time (in sec)	Generated Packets	Received packets	Packet Delivery Ratio	Throughput
30	840	670	0.7976	71.34
60	970	785	0.8093	72.38
90	983	810	0.8240	73.7
120	985	810	0.8223	73.55
150	985	810	0.8223	73.55
180	985	810	0.8223	73.55
210	985	813	0.8254	73.82
240	985	813	0.8254	73.82
270	920	795	0.8641	77.29
300	865	745	0.8613	77.03

Table-3: AODV with DoS Attack

Time (in sec)	Generated Packets	Received packets	Packet Delivery Ratio	Throughput
30	840	320	0.3809	36.07
60	970	390	0.4020	36.96
90	983	400	0.4069	39.95
120	985	406	0.4121	40.86
150	985	406	0.4121	42.77
180	985	408	0.4142	46.44
210	985	409	0.4152	48.76
240	985	409	0.4152	47.74
270	920	395	0.4293	46.67
300	865	370	0.4277	50.87

Throughput and Packet Delivery Ratio estimated was plotted in Fig-6 and Fig-7 respectively. From the graph it is evident that after a considerable amount of time the secure id method is close enough to services without DoS attack. The packet delivery ratio was remarkably improved, in a scenario where DoS attacks play a major role, with this method.

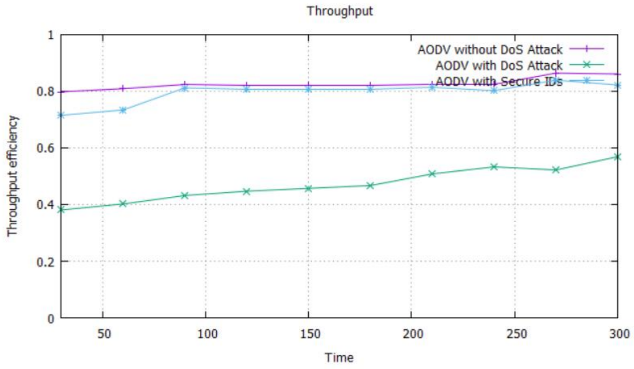

Fig-6: Throughput

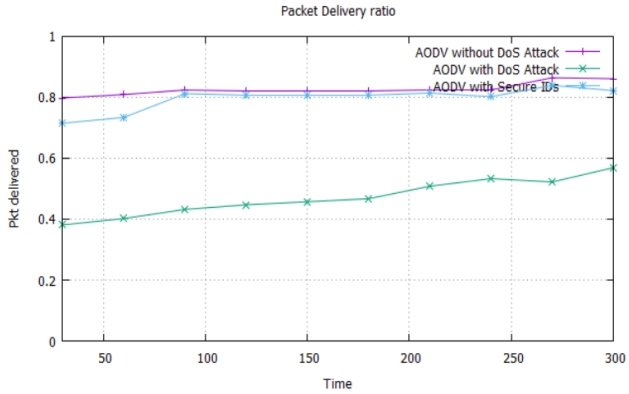

Fig-7: Packet Delivery Ratio

VII. CONCLUSION

Packet loss occurs in MANET/DANET due to several reasons such as wormhole attacks, black hole attack, grey hole attack, malware attacks etc. This can be prevented using encrypted network parameters linked with protocols, time of messages etc. for which intruders need remarkable amount of time for high density networks. Now a days, Denial of service attacks can't withstand for a long time since the identification parameters are increasing on various attributes including QoS. Our method helped to reduce data leakage in DANET using Homomorphic encryption methods applied on protocol level.

In our future work we plan to enhance the proposed scheme by considering more parameters that could be useful for evaluating the distributed denial of service attacks by making use of protocol steganographic methods.

REFERENCES

1. U. Gosh and R. Datta, "A Secure Addressing Scheme for Large-Scale Managed MANETs," in IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 483-495, Sept.2015. doi: 10.1109/TNSM.2015.2452292

2. A. Cavalli and J. Orset, “Secure hosts auto-configuration in mobile adhoc networks,” Ad Hoc Networks, vol. 3, no. 5, pp. 656–667, 2005.
3. M. Taghiloo, M. Dehghan, J. Taghiloo, and M. Fazio, “New approach for address autoconfiguration in manet based on virtual address space mapping(vasm),” in Proc. of IEEE ICTTA 2008, Damascus, Syria, 7–11 April 2008
4. X. Zou, Q. Li, SH. Sun, and X. Niu, The research on information hiding based on command sequence of FTP protocol, International, Proceedings Of The Th Systems, Conference On Knowledge-Based Intelligent, Springer, pp.1079–1085, 2005.
5. A. El-Atawy, and E. Al-Shaer, Building covert channels over the packet reordering phenomenon,In Proceedings of the 28th Annual IEEE Conference on Computer Communications (INFOCOM),IEEE, pp.2186–2194, 2009
6. B. Jankowski, W. Mazurczyk, and K. Szczypiorski, Information Hiding Using Improper Frame Padding, In Proc. of 14th International Telecommunications Network Strategy and Planning Symposium (Networks 2010), IEEE, pp.27–30, Warsaw, Poland, 2010.
7. K. Gai and M. Qiu, "An Optimal Fully Homomorphic Encryption Scheme," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 101-106. doi: 10.1109/BigDataSecurity.2017.43

AUTHORS PROFILE

Manoj Kumar G received his B.Tech Degree in Computer Science & Engineering from Kerala University and M.Tech degree in Computer Science & Engineering from Anna University. Currently, he is working as an Associate Professor in the Department of Computer Science & Engineering, LBS Institute of Technology for Women, Thiruvananthapuram affiliated to APJ Abdul Kalam Technological University. He is currently a research scholar at Karpagam Academy of Higher Education, Coimbatore. His areas of interest are Mobile Computing, Cryptography, Object Oriented Systems and Databases.

Prof. (Dr.) M. Abdul Rahiman is the Managing Director of Kerala State C-apt. He received the Doctor of Philosophy (Ph.D.) degree in Computer Science & Engineering from Karpagam University. He obtained his Master of Technology from Kerala University in 2004, and Bachelor of Technology from Calicut University. He achieved Post Graduate Diploma in Human Resource Management from Kerala University & Master of Business Administration. He is an eminent academician and an able administrator. He was the founder Pro Vice Chancellor of APJ Abdul Kalam Technological University and also served as Director, AICTE, Ministry of HRD, Govt. of India. He was also appointed as Director Vocational Higher Secondary Education to the Government of Kerala. He has also served as a Faculty of Engineering at LBS Institute of Technology for Women, Trivandrum. He specializes in Digital Image Processing & Pattern Recognition and he taught for more than 10 years having a rich teaching experience and current research areas are Image and Computer Vision, Data Mining and Networking. He is also serving as Member of many professional & technical bodies; chaired many Technical Conferences. Also serving in the Editorial board of many International Journals. He was also a Member of Advisory body of Technical Education UT of Daman Diu, which guides the Technical & Higher Education area.