CSRP: A Centralized Secure Routing Protocol for Mobile Ad Hoc Network

[1]Sourav Kumar Bhoi, [2]Imran Hossain Faruk, [3]Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology
Rourkela, India
[1]souravbhoi@gmail.com, [2]ihfaruk@gmail.com, [3]pmkhilar@nitrkl.ac.in

***Abstract*—Security in MANET is a grand challenge problem nowadays. The main security issues in MANET are identification and privacy. To combat with these problems, many secure routing protocols have been designed to reduce the security threats. In this paper, we have proposed a Centralized Secure Routing Protocol (CSRP) to enhance the security levels in the architecture to prevent the network against active and passive attacks. A Master Node (MN) is used in this architecture to control and manage the network security and data delivery. In the first step we have recognized the nodes and in the second step we have established session keys between the nodes for safe communication. The data delivery is done by encryption/decryption mechanism using session key. CSRP algorithm is mainly designed for secure and safe routing.**

Keywords-CSRP, MANET, Session Key, Master Node, Node Recognition

I. INTRODUCTION

MANET consists of wireless nodes which communicate with each other with the help of direct wireless links within range. This architecture has many functions like packet forwarding, routing, route discovery and security [14]. Security issues in MANET are a huge problem nowadays. The nodes are compromised and it is a threat to the MANET architecture. There are many type of attacks [10], [15] in MANET like active attacks and passive attacks. These are the most dangerous attacks to the MANET architecture which reduces and degrade the network performance [7]. So, security of data is the main issue in MANET architecture. The main security issues are privacy problem and identification problem. There are many secure routing protocols [1], [5], [6], [8], [9], [12], [13] which gives better solutions to these problems like ARAN, ARIDANE, LHAP, SAODV, SAR, SEAD, SLSP, SMT, SPARR, SRP, TESLA etc. CSRP provides solution to these two problems by identifying the genuine nodes taking part in the communication. In CSRP we have used the concept of digital signature and session key establishment to create a secure route for communication between the source and the destination. The first step here is to recognize the genuine nodes by the Master Node [17] and the second step presents the establishment of session keys [17] with the help of MN and delivery of data by encryption/decryption [11], [16], [17] process. The organization of the paper is as follows: section II presents the related work, section III presents the preliminaries, section IV presents the CSRP algorithm and section V presents about CSRP architecture and its performance. At last section VI presents the conclusion.

II. PRELIMINARIES

The main idea behind CSRP algorithm is its centralized architecture which consists of a MN which manages and controls the whole data communication and security in the network. Here, we have assumed MN as a genuine node and it is trusted by every other node. The idea of using MN in MANET is for enhancing the security. In CSRP algorithm MN helps in authenticating the nodes and helps in establishing session key between the nodes. Another assumption we have considered is the use of a third party (organization) which sets the general nodes in an area by placing a secret key S_K. S_K is common in MN and general nodes. It places the public keys e, n and hash function in MN and it also places the signature S in the general nodes. For example, if a malicious node wants to communicate or wants to enter into the area then it has to verify its identity which is easy for the MN to clearly identify the genuine node and imposter node. But if a genuine node wants to communicate or wants to enter into the network then it will easily pass the entity authentication [17] test. We have also assumed that there will be no physical tempering to the node so that no one damages or copy the code.

The use of digital signature in verifying the nodes and establishment of session key for data delivery are the key ideas used in CSRP.

III. PROPOSED CSRP ALGORITHM

A. Description

In our proposed CSRP algorithm, the main idea is to create a safe and secure route for data communication from source to destination. In CSRP architecture, we have taken the concept of Master Node and the general nodes. The key idea of using MN in MANET architecture is to provide a robust secure routing protocol. MN is used as a trusted third party which is used for authenticating the nodes. If a node wants to communicate with another node in MANET then the MN will generate a session key between them. For generation of session key between two nodes N_1 and N_2, N_1 has to send request to MN for establishing a session key K_{N1N2} with N_2 (neighbor). This process continues until we reach the destination. Then we flood the RREQ requests to the trusted neighboring nodes. Then we continue the process until we reach the destination. We consider the RREQ

which reach first and then we send a RREP from destination to source through the route taken by first RREQ. The data with the route as header is relayed by encrypting it with the session key of the two nodes and it is decrypted with the same session key on other end. This process continues till the destination is attained. This is how the data is relayed securely from source to destination.

B. Design

1) Node Recognition- The first step of CSRP algorithm is to recognize a node. This means, the nodes in an area set by the third party (organization) is to be recognized by MN to know whether the nodes are genuine nodes or malicious nodes. For this, organization places a pre-computed sign S and secret key S_K in the general nodes before placing the nodes in that area and it places a database of secret keys in MN. The public keys e, n and hash function are also placed in MN. S_K is common in MN and general nodes. For recognition of genuine nodes by MN it verifies the S_K first and then compute $h_1(S_K)=S^e \bmod n$. If the $h(S_K)$ matches with $h_1(S_K)$ then it verifies it as a genuine node and then MN changes the S_K and places it again in the node. S_K changes with time interval. This modification helps in securing the key safe.

Algorithm 1: Node Recognition

1. Same S_K is shared by MN and each node individually
2. MN knows the public key of signing algorithm
3. MN compute $h(S_K)$
4. Sign S is pre-computed and placed in the general node along with S_K
   $S = [h(S_K)]^d \bmod n$
   h = hash function known by both MN and general node
5. General node send request (S_K and S) to MN for verification
6. if (S_K (send by general node) = S_K (stored in MN))
   {
   $h_1(S_K) = S^e \bmod n$
   if ($h(S_K) = h_1(S_K)$)
   {
   Node is genuine
   }
   else
   {
   Malicious node
   }
   }
   else {
   Malicious node
   }
7. S_K changes with time interval

2) Connection Establishment and Secure Routing- The second step of our CSRP algorithm is to securely relay the data from source to destination. After recognizing the nodes by MN, the nodes establish session keys K_{N1N2} between themselves. If source want to send data to destination it establishes session keys between its neighbors and this process continues until we reach the destination. Then we check the Battery Power Status (BPS) of the nodes except source node and destination node. If BPS of a node is less than a threshold value (T) then RREQ request is not send to that node. By doing this we reduce the flooding of the packets, traffic in the network and power consumption. Then this process continues until we reach the destination and we choose the route covered by the first RREQ in the destination. Then a RREP is send from destination to sender and data delivery starts from source. Data delivery is done by encrypting the data with the session key and decrypting the data at other end. This encryption/decryption process continues and finally the data reaches the destination. If in case at the time of data delivery, an intermediate node fails then it searches for a new secure low cost route.

Algorithm 2: Centralized Secure Routing

1. After recognizing the nodes they will be the part of the network
2. Communication starts between source and the destination by establishing K_{N1N2} between the nodes.
3. Check the BPS of the nodes
4. if (BPS $\geq$ T)
   {
   Send RREQ requests to those nodes (flooding)
   }
5. RREQ flooding continues until the destination comes
6. Choose the first RREQ and send RREP through that route from destination to source
7. Data is relayed by encrypting the data by K_{N1N2} and decryption is done by the same K_{N1N2} at other end
8. Encryption/Decryption process continues until destination comes
9. End

IV. CSRP ARCHITECTURE & PERFORMANCE

CSRP gives a robust secure routing in the network. Here we have presented the working of CSRP and its performance with the help of an architecture. Figure 1 shows the CSRP architecture and the common secret keys which changes with respect to time. Table 1 shows the table of secret keys. Figure 2 shows how two nodes establish a session key. This process continues and every node establishes a session key with its neighboring nodes. Figure 3 presents that the key are established. After session key establishment the source node broadcasts RREQ and this process continues until RREQ reaches the destination. Then a RREP is send from destination to source from that route in which RREQ comes first. Then the data is delivered from the source in that route by encrypting it with the session key of two neighboring nodes in that route. Then this data is decrypted using the same session key and this process continues until the data reaches destination. Figure 4 shows the flooding of RREQ and RREP from D to S. Figure 5 shows the data delivery by encryption and decryption using session key. Figure 6 presents the end-to-end delay in sending data from source to destination. We know that MANET is hugely affected by Spoofing attack, Blackhole attack, Wormhole attack, Byzantine attack [10], [15] etc. which degrades the network performance. So, this architecture helps

in securing the data against these active and passive attacks and provides a secure routing [2], [3], [4] environment.

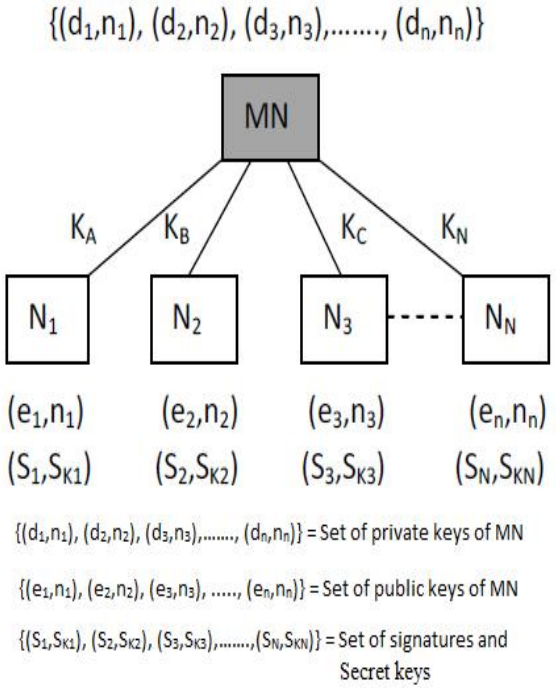

Figure 1. CSRP architecture with secret keys.

TABLE I. SECRET KEY TABLE

Used Secret Key	Changed Secret Key
S_{K1}	K_A
S_{K2}	K_B
S_{K3}	K_C
.	.
.	.
S_{KN}	K_N

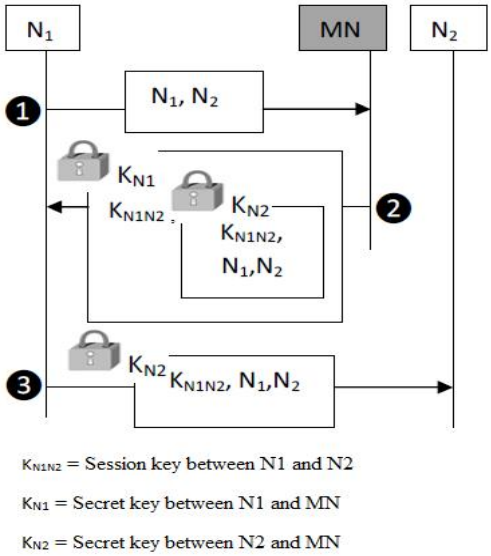

Figure 2. Session Key establishment.

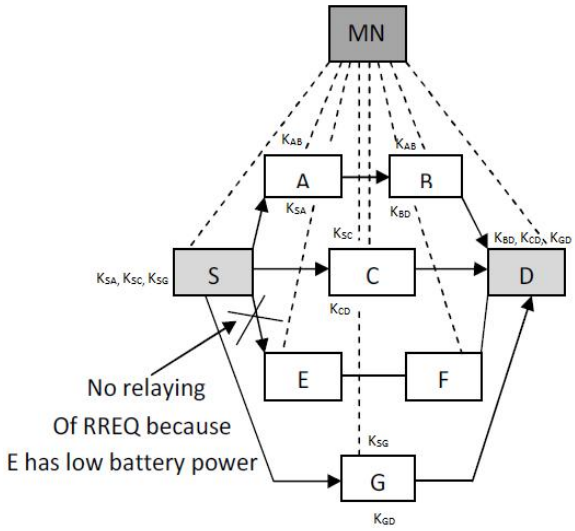

Figure 3. Session Key established between the nodes.

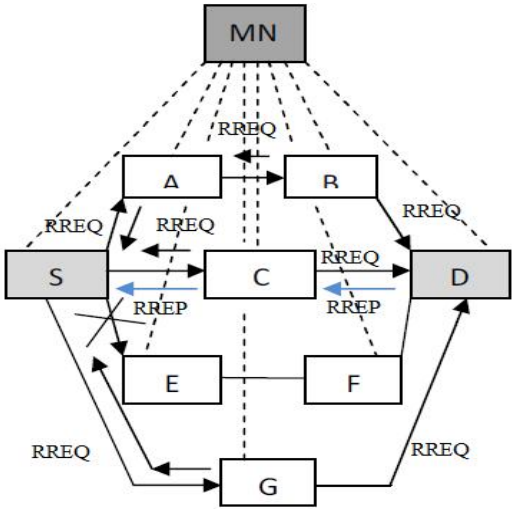

Figure 4. Flooding of RREQ to D and RREP from D to S.

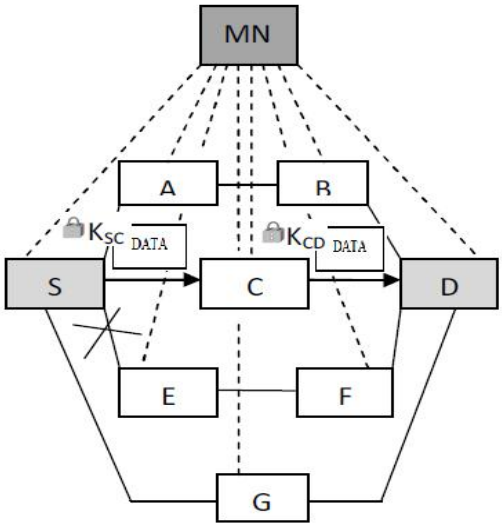

Figure 5. Data delivery by encryption and decryption using session key.

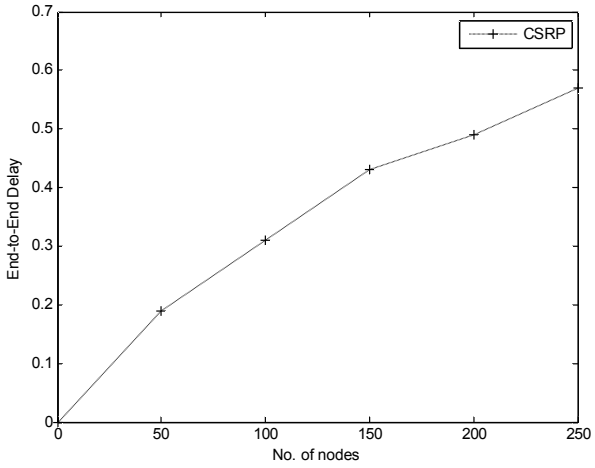

Figure 6. End-to-End Delay

V. CONCLUSION

CSRP algorithm shows better performance in finding a secure and safe route. CSRP's centralized architecture helps in controlling and managing the nodes in MANET. The use of digital signature and session key establishment in the algorithm provides better security with less computation. The use of BPS concept in the algorithm reduces the flooding of packets, traffic in the network and power consumption. So, CSRP provides a better security against active and passive attacks.

In future, we will implement the CSRP algorithm by showing better results. We will also work on the resistance of CSRP against different types of attacks.

REFERENCES

[1] M. Imani, M. Taheri, M. Rajabi, M. Naderi, "A Secure Method for a Routing Protocol in Ad Hoc Networks", International Conference on Educational and Network Technology, pp. 482-486, 2010.

[2] J. Liu, F. Fu, J. Xiao, Y. Lu, "Secure Routing for Mobile Adhoc Networks", Eighth ACIS International conference on Software Engineering, Arificial Intelligence, Networking and Parallel/Distributed Computing", pp. 314-318, 2007.

[3] D. Xiaojiang, S. Guizani, Y. Xiao, H. Chen, "NIS02-2: "A Secure Routing Protocol for Heterogeneous Network", IEEE GLOBECOM, pp. 1-5, 2006.

[4] S. Debideen, B. Smith, J. Garcia-Luna-Aceves, "An end-to-end solution for Secure and Survivable Routing", 7th International Workshop on Design of Reliable Communication Networks, pp. 183-190, 2009.

[5] R. Ramesh, S. Kumar, "Secure Position routing Using Ad hoc Network", International Conference on Ad Hoc and Ubiquitous Computing, pp. 200-201, 2006.

[6] M. Moustafa, M. Youssef, M. El-Derini, "MSR: A Multipath Secure Reliable Routing Protocol for WSNs, 9th IEEE/ACS International Conference on Comuter Systems and Applications (AICCSA), pp. 54-59, 2011.

[7] D. Kamboj, P.K. Sehgal, R. Nath, "Performance Evaluation of Secure Routing in Ad Hoc Network Environment", International Conference on Recent Advances in Information Technology, pp. 325-330, 2012.

[8] P. Ramachandran, A. Yasinsac, "Limitations of On Demand Secure Routing Protocols", Proceedings from the Fifth Annual IEEE SMC International Assurance Workshop, pp. 52-59, 2004.

[9] A. Modirkhazeni, N. Ithnin, O. Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", Second international Conferece on Network Applications Protocols and Services (NETAPPS), pp. 228-233, 2010.

[10] M. Yu, M. Zhou, W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environment", IEEE Transactions On Vehicular Technology, Vol: 58, Issue: 1, pp. 449-460, 2009.

[11] A. Mehmoud, A. Sameh, S. El-kassas, "Reputed Authenticated Routing for Ad Hoc Networks protocol (reputed-ARAN)", IEEE International Conference on Mobile Ad Hoc and sensor Systems, pp. 794-801, 2005.

[12] C. Lin, W. Lai, Y. Huang, M. Chou, "I-SEAD: ASecure Routing Protocol For Mobile Ad hoc Networks", International Conference on Multimedia and Ubiquitious Engineering, pp. 102-107, 2008.

[13] N.H. Saeed, M.F. Abbod, H.S. Al-Raweshidy, "MANET Routing Protocols Taxonomy", International Conference on Future Communication Networks (ICFCN), pp. 123-128, 2012.

[14] R. Seikh, C. Singh, D. Mishra, "Security Issues in MANET: A review, " Seventh International Conference On Wireless and Optical Communications Networks (WOCN), pp. 1-4, 2010.

[15] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, " A Survey of Routing Attacks in Mobile Ad Hoc Networks", Wireless Communications, IEEE, Vol:14, Issue:5 , pp. 85-91, 2007.

[16] K. Shin, Y. Kim, Y. Kim, "An effective Authentication Scheme in Mobile Ad Hoc Network", Seventh ACIS International conference on Software Engineering, Arificial Intelligence, Networking and Parallel/Distributed Computing, pp. 249-252, 2006.

[17] B. Forouzan, D. Mukhopadhya, "Cyrptography and Network Security", 2nd Edt. , Tata Mcgraw Hill Pvt. Ltd., ISBN: 007070208X, 2011.