Available online at: http://www.ijmtst.com/vol6issue06.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 06, Issue No: 06, June 2020

Security of Data with Enhanced Technique of AASR Protocol for Secure Crosslayer Routing in MANET

Shifana Begum[1] | Megha M Gamskar[2] | Prakrithi Mogasale[2]

[1]Assistant Professor, Dept. of CSE, Srinivas School of Engineering, Mangalore, Karnataka, India.

[2]UG Student, Dept. of CSE, Srinivas School of Engineering, Mangalore, Karnataka, India

To Cite this Article

Shifana Begum, Megha M Gamskar and Prakrithi Mogasale, "Security of Data with Enhanced Technique of AASR Protocol for Secure Crosslayer Routing in MANET", *International Journal for Modern Trends in Science and Technology*, Vol. 06, Issue 06, June 2020, pp.:17-21; https://doi.org/10.46501/IJMTST060605

Article Info

Received on 27-April-2020, Revised on 23-May-2020, Accepted on 23-May-2020, Published on 30-May-2020.

ABSTRACT

MANET supports communication without any wired medium and with layered architecture. It does not uses any infrastructure support. Present alternative to the layered architecture is cross layer design approaches and the interaction between the layers is supported. The security of CLPC (Cross Layer Design Approach for Power control) routing protocol will be discussed in this paper. The transmission power and finding the effective route between source and destination can be improved by CLPC. The reliable path between the source and destination can be determined by RSS from the physical layer, but it is vulnerable to the DOS attacks. Here we propose a Secure cross layer power control protocol SCLPC to placate the attacks on CLPC. The SCLPC protocol provides better results and performance.

KEYWORDS: MANET, CLPC, SCLPC, RSS, AASR Protocol and Onion Routing.

DOI: https://doi.org/10.46501/IJMTST060605

I. Introduction

MANET Mobile Adhoc Network is a dynamic, decentralized and also an infrastructure less network which we use for communication. Here destiny can vary and mobility speed can be high[1]. The challenging issues for MANET are battery constraints, high mobility, link breakage and limited bandwidth.

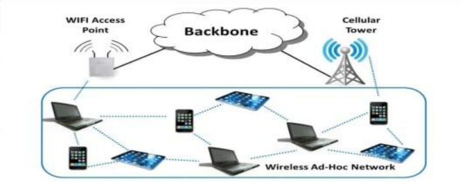


Figure 1: Mobile Ad Hoc Network (MANET)

The architecture here which is layered allows the designer to target only specific parameter which is limited to the layer. But as we see in cross layer design the parameter of one layer can be interfaced with the other layer. It also provides the cross layer optimization and QOS [2]. The Cross layer based approach will provide better results but the security of cross layer based designs is challenging issues. The various network parameters can be affected by the transmission power control issues. The security model SCLPC is proposed that is based on anonymity and authentication. Anonymous communication means identities of source and destination nodes cannot be revealed to other nodes also the link or traffic between source and destination cannot be recognized by any other node [4]. Nodes are aliased with pseudonym. To defend any type of attacks and to prevent the intermediate nodes from modifying the packets, RREQ packets are authenticated by group signature and key encrypted onion routing with route secret verification message is designed to prevent the intermediate nodes from inferring as destination.

II. LITERATURE SURVEY

Sreedhar C., Dr. S. Madhusudana Verma, Dr. S. Kasiviswanath [6] proposed cross layer based secure routing protocol CSR-MAN. They implemented interaction of Physical layer, MAC layer and Network layer. By calculating RSS value at physical layer, node then calculates the available bandwidth at MAC layer.

Suresh Babu and K. Chandra Sekharaiah [5] implemented CLDASR (Cross layer based detection and authentication technique for secure multipath routing) protocol against the network layer attack i.e. black hole, gray hole. In the authentication method, when a source wants to send a data packet symmetric key with the destination. In the black hole or grayhole detection method, every node observes the next hope in the current route path.

Azza Maohammed, Boukli Hacene Sofiane and Faraoun Kamel Mohamed [7] propose CrossAODV as a secure cross layer routing protocol with cross layering of MAC layer and Network layer. They suggested the verification and validation of routing information through RTS/CTS frame.

R. Madanmohan and K. Selvakumar proposed a cross layer design approach for power control.

Joseph Soryal, Tarek Saadawi proposed a mechanism for endto-end Cross Layer Design protocol in a totally distributed environment to detect and react to DoS attacks targeting IEEE 802.11 MAC layers.

III. Cross Layer Design Framework With Malicious Behavior

In Cross layer design, the nodes collects the RSS (Received Signal Strength) values from their by broadcasting a message packet. By using dynamic transmission power control mechanism, every node calculates minimum RSS, Average RSS and Maximum RSS. Then the source node generally selects the nodes with a minimum distance from it and having maximum RSS value. Nodes with maximum RSS value are considered as more durable and reliable and depending on RSS values the routing decision are made. In this each node calculates the Average of all its neighbors RSS as and define three threshold as shown in Table 1. Using these values every node determines the communication region and source nodes arrange the nodes region wise based on node's RSS value. Source nodes broadcast the RREQ to nodes on Maximum communication region and intermediate nodes determines the RSS to decide whether or not to broadcast it to the next node.

RSS	**Equation**	**Condition**
A_RSS	$=\sum^{n}_{i=1}RSSi/n$	-
A_Min_RSS	$=\sum_{i=1}^{MIN\_NODE} RSS_i /Min\_Node$	RSS_i<A_RSS
A_Max_RSS	$=\sum_{i=1}^{MAX\_NODE} RSS_i/Max\_Node$	RSS_i>A_RSS

Table 1: Thresholds for Average RSS values

IV. Proposed Routing protocol

As mentioned above under malicious behaviour CLPC has been occurred with less performance metrics. It has been proved that Cross layer design protocols [10] are better but security of such protocols is important and we should detect and mitigate the attacks. In this paper we have attempted to implement AASR (Authenticated Anonymous secure routing) protocol. The SCLPC works as mentioned in the steps :

(i) Every node can collect the neighbours RSS by broadcasting hello packets and compute the threshold value as discussed in section 3. It is difficult for attacker to measure the individual RSS values of nodes. (ii) At Routing layer, a node from Maximum communication region with RSS > A_RSS along with verified group signature key is selected for broadcasting the RREQ. (iii) Attacker cannot modify these RSS values and we can keep all the anonymous by assigning the pseudonyms. (iv) For intermediate nodes we are using key encrypted onion routing with route secret verification message from inferring as destination. The RSS can be computed by MAC layer and using dynamic transmission control power it is updated in routing table of node timely. If we succeed to keep the source, destination, route of transmission and RREQ and RREP packets anonymous then we can able to mitigate the attacks strongly.

A. *Network Assumption*

Let T represents the MANET network then following are the assumptions for anonymous routing:

1) NSK(Neighborhood Symmetric Key): By making use of their public/private keys, any two nodes in a neighborhood can establish a security association and create a symmetric key .

2) PKI (Public Key Infrastructure): In this, the each node T initially has a pair of public or private keys issued by a public key infrastructure(PKI) or other certificate authority (CA).

3) The Group Signature: Here the entire network T is considered as a group and each node has a pair of group public or private keys issued by the group manager. The group public key is the same for all the nodes in T, while the group private key is different for each node.

B. *Onion Routing*

It is a mechanism to provide private communication over a public network. In an onion network, messages are encapsulated in layers of encryption, resembling the layers of an onion. Then encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination and the process continues until the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes. The intermediate nodes can verify its role by decryption and deleting the outer layer of the onion. Eventually, an anonymous route can be established.

C. *Protocol Design*

AASR is adhoc on demand based routing protocol with functions of route discovery, data transmission and route maintenance. We implemented AASR in SCLPC (Secure Cross Layer based Power control Protocol).

The design of protocol is as follows.

1) Every node computes RSS value of its adjacent nodes and formulates three regions depending on RSS value.
2) After computing the RSS from neighbour, source node S initiates route discovery to find its destination D. S forwards RREQ to nodes belonging to maximum communication region with RSS > A_RSS.
3) When RSS is high nodes are nearer to each other of generally 1-hop distance. We assume source S knows destination D. Following Procedure is performed by SCLPC.

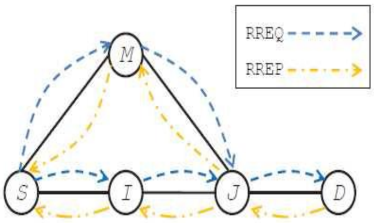


Figure 2: Network Topology

V. Implementation

The implementation was performed using JAVA J2EE to compare the performance of SCLPC against the MCLPC (CLPC with malicious behaviour). The AASR (Authentication Anonymous secure routing) protocol hides the details of source, destination nodes. SCLPC selects the nodes from maximum communication region for broadcasting the packets. It selects the node with max RSS from maximum communication region and who are authenticated with group signature keys. This provides security overall network. Pseudonym used for source id, destination id and packets makes the attacker difficult to identify and track the network flow. There are three performance metrics within this designed implementation that are related to the modified and proposed algorithms in this thesis, which they are:

- Delay (End-to-End): It is the delay time elapsed to send a specific size of data from the source node until reaching to the destination node.
- Packet Delivery Ratio (PDR): It is the ratio of the traffic received to the traffic sent in the network.
- Throughput: It is measure used to determine the rate of successful data delivered to destination node over the communication channels in network.

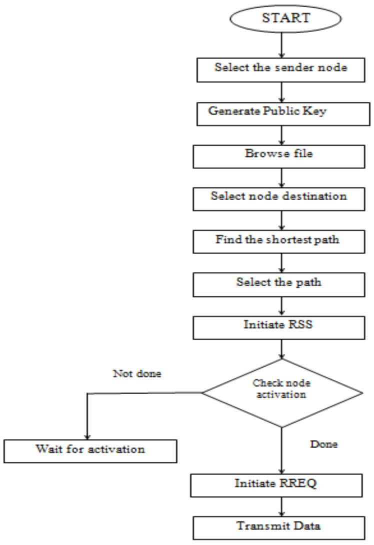


Figure 3: Flow diagram of Sender side

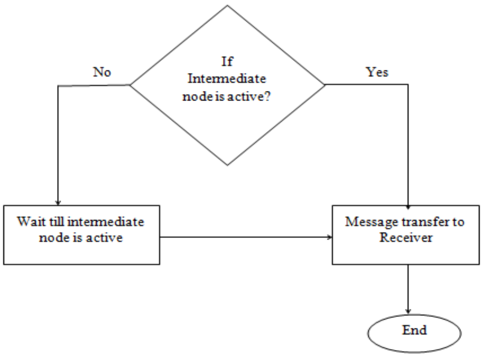
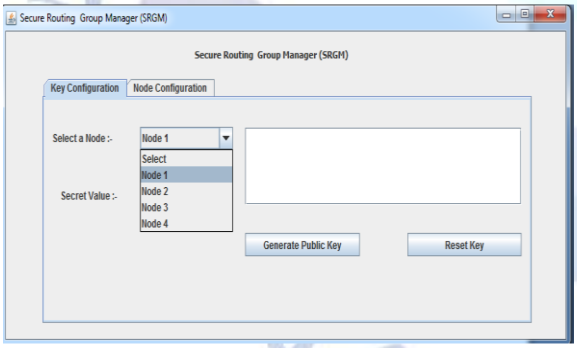

If Intermediate node is active?
No
Yes
Wait till intermediate node is active
Message transfer to Receiver
End

Figure 4: Flow diagram of Receiver side

VI. RESULTS



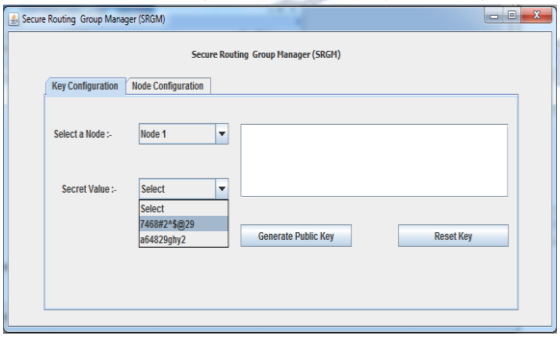
Secure Routing Group Manager (SRGM)

Select a Node :- Node 1

Select
Node 1
Node 2
Node 3
Node 4

Secret Value :-

Figure 5: Selecting a node in Key Configuration



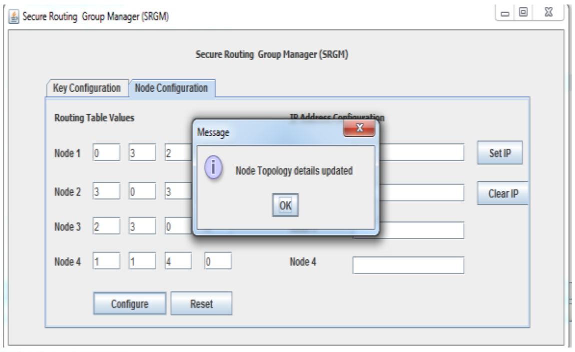
Secure Routing Group Manager (SRGM)

Select a Node :- Node 1

Secret Value :- Select

Select
7468#2^$@29
a64829ghy2

Figure 6: Selecting a secret key in Key Configuration



Secure Routing Group Manager (SRGM)

Routing Table Values

IP Address Configuration

Node 1 0 3 2

Node 2 3 0 3

Node 3 2 3 0

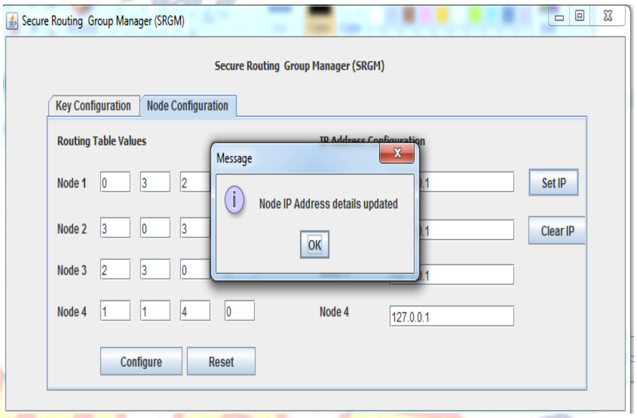
Node 4 1 1 4 0

Node 4

Message

Node Topology details updated

Figure 7: Updating Routing table in Node Configuration



Secure Routing Group Manager (SRGM)

Routing Table Values

IP Address Configuration

Node 1 0 3 2

Node 2 3 0 3

Node 3 2 3 0

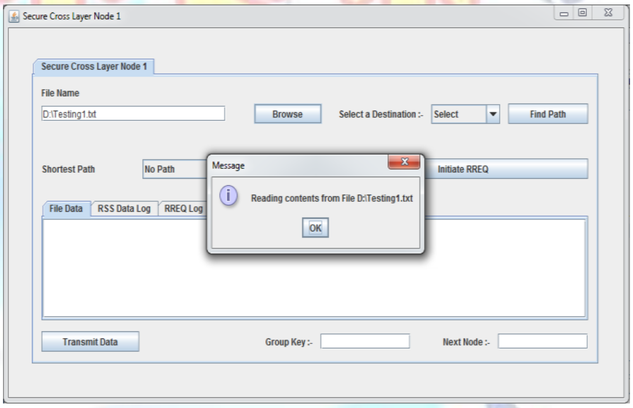
Node 4 1 1 4 0

Node 4 127.0.0.1

Message

Node IP Address details updated

Figure 8: Updating Node IP addresses



Secure Cross Layer Node 1

File Name D:\Testing1.txt

Select a Destination :- Select

Shortest Path No Path

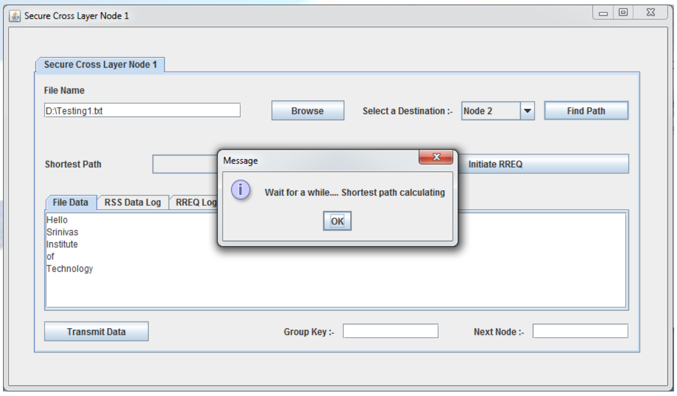
Group Key :-

Next Node :-

Message

Reading contents from File D:\Testing1.txt

Figure 9: Browsing and Selecting a file for Transmission



Secure Cross Layer Node 1

File Name D:\Testing1.txt

Select a Destination :- Node 2

Shortest Path

Hello
Srinivas
Institute
of
Technology

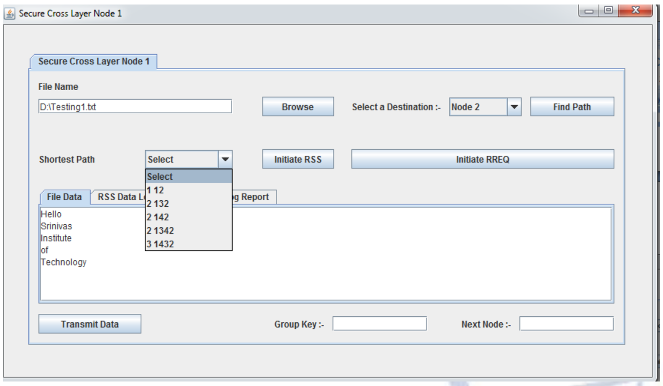
Group Key :-

Next Node :-

Message

Wait for a while.... Shortest path calculating

Figure 10: Selecting Destination node and finding a path



File Name: D:\Testing1.txt

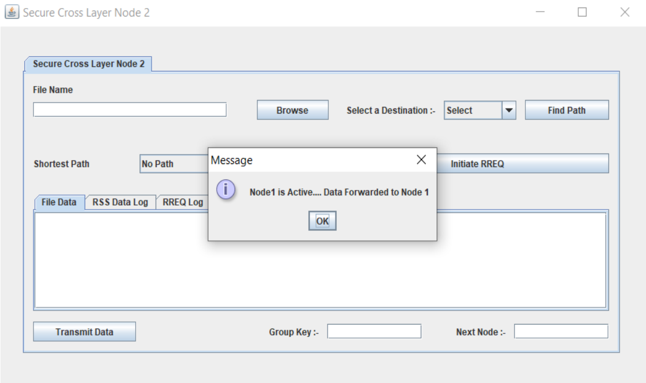
Select a Destination :- Node 2

Shortest Path: Select

Select
1 12
2 132
2 142
2 1342
3 1432

Hello
Srinivas
Institute
of
Technology

Figure 11: Selecting Shortest path and Initiating RSS

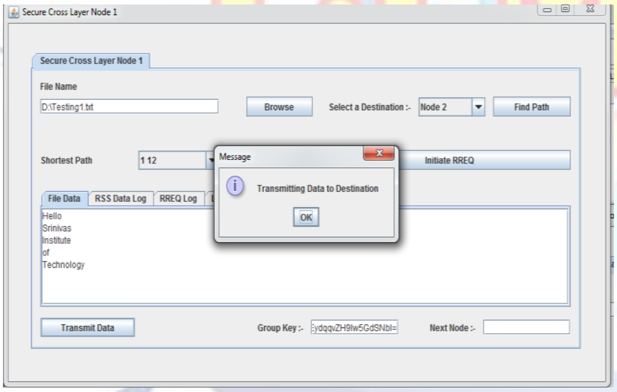


Select a Destination :- Select

Shortest Path: No Path

Node1 is Active.... Data Forwarded to Node 1

Figure 12: RSS value is received by Destination node



File Name: D:\Testing1.txt

Select a Destination :- Node 2

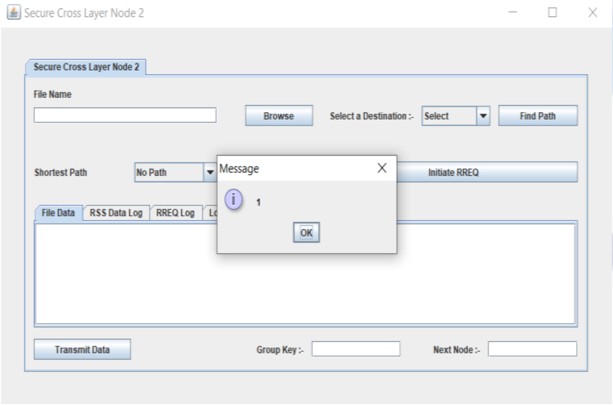
Shortest Path: 1 12

Transmitting Data to Destination

Hello
Srinivas
Institute
of
Technology

Group Key :- :ydqqvZH9lw5GdSNbl=

Figure 13: Transmitting data from Source node

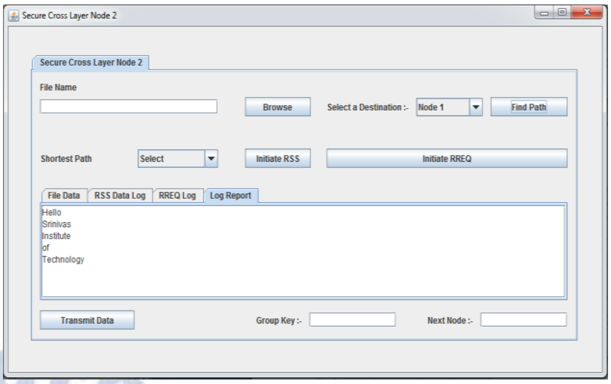


Select a Destination :- Select

Shortest Path: No Path

1

Figure 14: Data is received by Destination node



Select a Destination :- Node 1

Shortest Path: Select

Hello
Srinivas
Institute
of
Technology

Figure 15: received data is displayed in Log Report

VII. Conclusion and Future Works

CLPC protocol is cross layer based protocol designed to overcome the problem of link breakage. CLPC is giving optimum performance but for malicious attack, the performance is under influence and attacker can disrupt the network functions. Hence the objective of designing the SCLPC is to provide secure and reliable routing service for MANET using cross layer design to mitigate various attack. To defend such attacks we proposed solution using AASR protocol and as shown in implementation results SCLPC has better performance. Future work is to achieve the optimum performance as imposed security using anonymous routing incurs the routing load and increased the end to end delay.

Future work may include more experiments on MANET for other Routing Protocols. In future work may include more experiments on MANET for other Routing Protocols. Further study should be assigned to implement a more Reliable and Integrated System, where we can have different Nodes together and the System can automatically be able to select the Protocol and Algorithm, necessary to provide a High level of Security.

References

[1] Amit A Bhusari "Review and Classification for cross layer Routing protocol for MANET".

[2] Vineet Srivatsa "Cross Layer design a survey and road ahead".

[3] A sarfaraz ahmed "Cross Layer Design approach for power control."

[4] Vey Liu "Authenticated Anonymous secure routing for Manets in adversarial environments".

[5] K suresh chandra "CLDASR in MANET".

[6] Sreedhar C "Cross Layer based secure routing in MANET".

[7] Azza Mohammed "A cross layer for detection and ignoring backhole attack in MANET".