International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Volume 1 Issue 4 (October 2014) ISSN: 2349-7009(P)
www.ijiris.com

SRAAA – Secured Right Angled and Ant Search Hybrid Routing Protocol for MANETs

Capt. Dr. S. Santhosh Baboo
Associate Professor
D G Vaishnav College, Chennai

V J Chakravarthy
Research Scholar
D G Vaishnav College, Chennai

Abstract— This paper is a contribution in the field of security analysis on mobile ad-hoc networks, and security requirements of applications. Limitations of the mobile nodes have been studied in order to design a secure routing protocol that thwarts different kinds of attacks. Our approach is based on the Right Angled and Ant Search Hybrid Routing Protocol (RAAA); the most popular hybrid routing protocol. The importance of the proposed solution lies in the fact that it ensures security as needed by providing a comprehensive architecture of secured Right Angled and Ant Search Hybrid Routing Protocol (SRAAA) based on efficient key management, secure neighbor discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network. In order to fulfill these objectives, both efficient key management and secure neighbor mechanisms have been designed to be performed prior to the functioning of the protocol. To validate the proposed solution, we use the network simulator NS-2 to test the performance of secure protocol and compare it with the conventional zone routing protocol over different number of factors that affect the network. Our results evidently show that our secure version paragons the conventional protocol in the packet delivery ratio while it has a tolerable increase in the routing overhead and average delay. Also, security analysis proves in details that the proposed protocol is robust enough to thwart all classes of ad-hoc attacks.

Keywords— Black hole attack, Secure level, Secure based routing protocol, performance analysis

I. INTRODUCTION

In MANETs the nodes are free to move in any route and arrange themselves randomly. They can be a part of or keep the Network at any time. Due to the regularly modify in the Network topology there is a important modify in the position of Secure in among different nodes which contributes the complexness to redirecting among the various Mobile nodes. The self-organization of nodes in ad hoc Networks may to refuse offering services for the benefits of other nodes in order to keep their own sources familiarize new protection that are not resolved in the infrastructure-based Networks in MANET. Routing methods for MANETs are usually categorized into practical and sensitive methods, and MANETs methods depending on how redirecting details is obtained and managed by Mobile nodes. Desk practical methods use a practical redirecting plan, in which every Network node preserves reliable up-to-date redirecting details from each node to all other nodes in the Network. On-demand-reactive methods are depending on a sensitive redirecting plan, in which at least one direction is recognized only when required. A MANETs redirecting method is a mixture of practical and sensitive techniques with the aim of taking benefits of the key benefits of both types of methods. AODV is other redirecting criteria used in ad hoc Networks, it does not use resource redirecting, but it is on-demand [2]. In ES-AODV, each node preserves a redirecting table which is used to shop location and next hop IP details as well as location series figures [3]. The attractive features of ad-hoc networks such as open medium, dynamic topology, absence of central authorities, and distributed cooperation hold the promise of revolutionizing the ad-hoc networks across a range of civil, scientific, military and industrial applications. However, these characteristics make ad-hoc networks vulnerable to different types of attacks and make implementing security in ad-hoc network a challenging task. The main security problems that need to be dealt with in ad-hoc networks include: the identity authentication of devices that wish to talk to each other, the secure key establishment of keys among authenticated devices, the secure routing in multi-hop networks, and the secure transfer of data [16]. This means that the receiver should be able to confirm that the identity of the source or the sender (i.e., one hop previous node) is indeed who or what it claims to be. It also means that the receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit. In this paper, we propose securing one of the most popular hybrid protocols: Right Angle and Ant search routing protocol (RAAA). For details on the basic operation of RAAA, Conventional RAAA is not secure and does not consider security requirements. First, we use an efficient key management mechanism that is considered as a prerequisite for any security mechanism. Then, we provide a secure neighbor detection scheme that relies on neighbor discovery, time and location based protocols [18]. Securing routing packets is considered as the third stage which depends on verifying the authenticity of the sender and the integrity of the packets received. Finally, detection of malicious nodes mechanism is used to identify misbehaving nodes and isolate them using blacklist. Once these goals are achieved, providing confidentiality of transferred data becomes an easy task which can be implemented using any cryptography system.

II. RELATED WORKS

The mobile ad hoc systems are self developing, self providing and planning organizations. We present research on the actions of the Practical Redirecting Strategy in the Lines by research of various factors. The Efficiency analytics that are used to assess routing techniques are Bundle Distribution Rate (PDR), System Control Expense, Stabilized Expense, Throughput and Regular End to End delay on [3]. Shortest path algorithm is a simple and clear and understandable method. In primary design of this method to create a chart of the subnet, with each node of the chart in place of a radio router and each posture of the chart comprising a concept line using weblink. For result a direction between a given couple of wireless routers, the criteria just discovers the shortest direction between them on the chart. The duration of a direction can be calculated in various ways as on the reasons for the variety of trips, or on the reasons for area range [1]. They have more using the routing strategy to applying for a details transmitting on the system. The solution discovers the traffic happened nodes and isolates it from the effective details sending. Since suggested Multiple routing is used to identify and eliminate traffic at physical part using hop depend and adjustment of AODV protocol using direction reaction decision and lastly we using protected next door neighbor finding using next door neighbor list method [6]. These techniques are mixed to acquire the control remedy which is for better then individual techniques. These hybrid routing is based on ON-Demand ad hoc routing protocol (AODV).Security strikes in MANET routing can be separated in network performance design on objective of a strike is generally to pay attention and recover important details inside details packages, for example by releasing a traffic tracking strike. In such an strike, a harmful node tries to recognize interaction events and performance which can offer details to release further strikes [7]. The strike type is known as inactive since the regular performance of the network is not changed. That time to recognize the strike design, so we have using the protected and effective routing protocol and then preventing design of their process. The direction finding starts with the surging of Route Requirement (RREQ) information by a resource node. RREQ is transmitted from resource S, obtained by the next neighbor nodes of S, and then is rebroadcast. This Multihop transmitting allows the RREQ to achieve the predicted location D. In reaction to the RREQ, D unicast Route Reply (RREP) information toward S. This RREP will gradually achieve the resource node through the Multihop direction. In this way, the direction from S to D is recognized [15]. It should be mentioned that this direction is the shortest direction out among possible tracks, and is best direction performance on their network. Multiple routing techniques [6] aggregates a set of nodes into areas in the network topology. Then, the network is portioned into areas and proactive strategy is used within each area to sustain routing details. To direction packages between different areas, the sensitive strategy is used. Consequently, in hybrid techniques, a direction location that is in the same area is recognized straight away, while a direction finding and a direction servicing process is required for locations that are in other areas [7]. The routing protocol offer a bargain on scalability issue in regards to the regularity of end-to-end relationship, the depend of nodes, and the regularity of topology change.

III. SRAAA SECURITY REQUIREMENTS

The following security requirements are to be satisfied by SRAAA.

A. Detection of malicious nodes:

If there are malicious nodes in a network, then SRAAA should be able to detect them and avoid choosing such nodes during the routing process.

B. Authentication:

It is fundamental to verify the identity of hybrid ad hoc wireless network node and its fitness to access the network. In other words, nodes that wish to communicate with each other must ensure that they are communicating with the right party and that they are genuine, not impersonators. SRAAA must ensure that data is from the origin and not modified or falsified.

C. Authorization:

The nodes in hybrid ad hoc wireless networks need to have accurate authorization in order to access shared resources on the network. SRAAA ensures that only authorized nodes are allowed to enter the network, store information and use it on their devices.

D. Confidentiality:

The information that is sent between the hybrid ad hoc network nodes resident on their devices, or related to their locations, needs to be protected. SRAAA ensure that the data which has been sent between the nodes is the same and has not been modified, deleted or retransmitted to another node or entity.

E. Availability:

The availability of a network means that its essential services and applications should be accessible at any time when they are needed, even in the event of a breach in security. With this availability, SRAAA ensures the survivability of the network, despite malicious attacks or the misbehavior of particular nodes. This requirement is especially important in

hybrid ad hoc wireless networks, where security breaches, attacks and malfunctions are more frequent and less likely to be detectable

F. Data integrity:

The information that is exchanged between the nodes needs to be protected in order to ensure that messages by SRAAA, which have been sent are the same and have not been modified, deleted or retransmitted to another node or entity. This is most fundamental in situations such as banking, military operations and equipment controls, where such modification or deletion could cause potential damage.

G. Guarantee of secure correct route discovery:

SRAAA ensures that the protocol is able to find the route correctly and provide security for the selected route.

IV. SRAAA MECHANISM

Our main focuses are to introduce SRAAA to protect data transmission and to construct a secure routing protocol.

Our SRAAA approach uses a hybrid of security mechanisms so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash function, Certificates, time synchronization and route discovery request.

SRAAA works as a group and has Four stages, examined in turn in the remainder of this section:

A. Route Request Process:

1. Route Request message MD5 encryption by Destination
2. Send Encrypted Route Request Message with Symmetric key from Destination with unique ID (MAC Address)
3. Decrypting MD5 by source and check the route request

B. Detect and Eliminate the Attackers from The Routing table Process:

1. Detecting Attackers in the network by looking up duplicate requests
2. Removing those nodes from the routing table

C. Certificate Distribution to all the authenticated nodes:

1. Source Generates and distribute the Certificates to all the authenticated nodes

D. Packet Transfer Process:

1. Sending Packets to the proper destination with SES data encryption technique
2. Receiving packets and SES decryption by destination

V. WORKING PRINCIPLE OF SES (SECURED ENCRYPTION SYSTEM) ALGORITHM

SES (Secured Encryption system) algorithm uses Symmetric-keys that are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more nodes that can be used to maintain a private information link. Both the nodes have the access to the secret key. The key size used for an SES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

10 cycles of repetition for 128-bit keys.
12 cycles of repetition for 192-bit keys.
14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key, tables as shown in Table 1.

TABLE 1 HIGHLIGHTS THESE CATEGORIES OF DATA

128-Bit Key Avalanche
Plaintext Avalanche
Plaintext/Cipher text Correlation
Cipher Block Chaining Mode
Random Plaintext/Random 128-Bit Keys
Low Density Plaintext
Low Density 128-Bit Keys
High Density Plaintext
High Density 128-Bit Keys

VI. WORKING PRINCIPLE OF MD5 MESSAGE-DIGEST ALGORITHM:

"MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. MD5 is considered one of the most efficient algorithms currently available and being used widely today.

MD5 algorithm uses four rounds, each applying one of four non-linear functions to each sixteen 32-bit segments of a 512-bit block source text. The result is a 128-bit digest. Below is a graph representation that illustrates the structure of the MD5 algorithm.

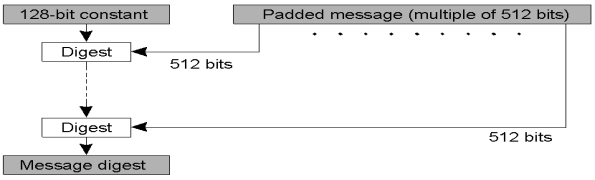


Fig. 1 Structure of MD5 algorithm

MD5 algorithm takes a b-bit message as input, where b is an arbitrary nonnegative integer. The following five steps are performed in C programming language to compute the message digest of the input message.

Step1. Append padding bits

The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512. Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. In all, at least one bit and at most 512 bits are appended.

Step2. Append length

A 64-bit representation of b (the length of the message before the padding bits were added) is appended to the result of step1. If b is greater than 2^64, then only the low-order 64 bits of b are used. (These bits are appended as two 32-bit words and appended low-order word first in accordance with the previous conventions.) The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words. Let M [0 ... N-1] denote the words of the resulting message, where N is a multiple of 16.

Step3. Initialize MD buffer

A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step4. Process message in 16-word blocks

Four auxiliary functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z
G (X, Y, Z) = XZ or Y not (Z)
H (X, Y, Z) = X xor Y xor Z
I (X, Y, Z) = Y xor (X or not (Z))

In each bit position, F acts as a condition such that if X then Y else Z. The function F could have been defined using "addition" instead of "or" since XY and not (X) Z will never have 1's in the same bit position.

The functions G, H, and I are similar to the function F, which performs in "bit-wise parallel" to produce its output from the bits of X, Y, and Z so that if the corresponding bits of X, Y, and Z are independent and unbiased. Therefore, each bit of G (X, Y, Z), H (X, Y, Z), and I (X, Y, Z) will be independent and unbiased.

This step uses a 64-element table T [1 ... 64] constructed from the sine function. Let T [i] denote the i-th element of the table, which is equal to the integer part of 4294967296 times abs (sin (i)), where i is in radians. Then, performs the 4 rounds of hashing for each 16-word block:

VII. RAAA ROUTE RECORD

Each node in the network which contributes to setting up the route or which is involved in forwarding the data packet to the destination has a record in the list, which is constructed during the stage of finding the path to the destination. An additional task of this list is to share with the destination the sequence numbers, preventing the counting-to-infinity problem. The field names of the Route record used in the developed approach , tables as shown in Table 2.

TABLE 2. RAAA Route Record

Field Name	Description
lr_nodeIP	Node IP address
lr_nodedir	Node heading angle
lr_nodeSL	Stability of link

A. Route Request Message Format:

If the destination node is not a neighbour to the source node, the route request message is initiated and prepared by the source node with the necessary information before being transmitted onto the network. The fields most commonly required in the RREQ message are the source and destination IP addresses, the RRL and the packet type (to differentiate between route request, route reply, route error, acknowledgment and hello messages). The general field names used in the RREQ message, tables as shown in Table 3.

TABLE 3. Route Request Message Format

Field Name	Description
rq_type	Packet Type
rq_bcast_id	Broadcast ID
rq_dst	Destination IP Address
rq_dst_seqno	Destination Sequence Number
rq_src	Source IP Address
rq_src_seqno	Source Sequence Number
rq_timestamp	When RREQ sent
rq_rt_list	Route Record List

B. Route Reply Message Format

The route reply message is initiated and prepared with necessary information by the destination node or by an intermediate node, which has a fresh enough route to the destination node. The RREP is then unicast back to the source node that generated the RREQ. In our developed scheme, the RREP message consists of identical fields. In general, the main fields required in the RREP message are the source and destination IP addresses the RRL and the packet type. Here, it is important to notice that the Destination MAC Address field refers to the node that generates the RREQ message and the message will be getting encrypted by MD5 technique. while the Source IP Address field denotes the node that generates the RREP message. The general field names used in the RREP message, tables as shown in Table 4.

TABLE 4. Route Reply Message Format

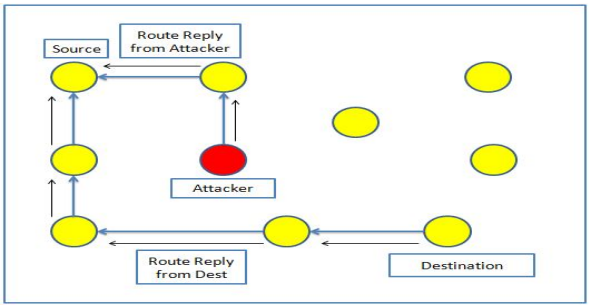
Field Name	Description
rp_type	Packet Type
rp_dst	Destination IP Address
rp_dst_mac	Destination Mac Address
Rp_Md5_Enc	MD5 Encryption message

rp_dst_seqno	Destination Sequence Number
rp_src	Source IP Address
rp_lifetime	Lifetime
rp_timestamp	When corresponding RREQ sent;
rp_rt_list	Route record list

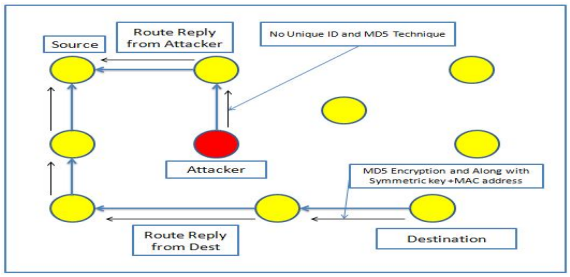
Pseudo Code:

Algorithm 1: Pseudo-code for SRAAA mechanism
Source Broadcasts RREQ packet
Destination and Attackers Send RREP
If RREP packet received then
Decrepit the Reply message with MD5 and Symmetric key and Mac Address
Find the Attackers
Eliminate from Routing Table
Find Multi path to the destination with RAAA
Sends data packets to destination in smart route

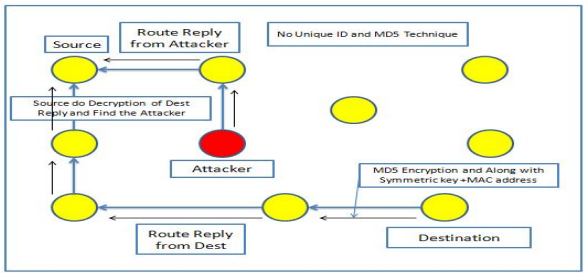
The Evaluation of SRAAA from RAAA:
Step 1- A Source node need a route to destination it broadcast a Hello packet across the Network.
Step 2- Any node receiving this packet update their
Step-1 A source node need a route to destination in broadcast a Hello packet across the network.
Step-2 A node receiving this pacet update their information for the source node and Will do following.
2.1: If <Source address, Req id> is found in this node then discard the Route Request packet.
2.2: If the node address listed in the Route Record. Discard the Route Request Packet.
2.3: If the target of the Request node match this host address return a copy of this route in a Route replies Packet to the source node.



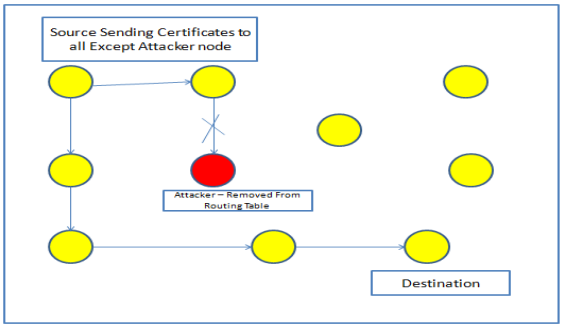
2.4: Proper Destination sends the Route Reply packet with Symmetric key with MD5 Encryption
2.5: Attackers also sends a route reply but without Encryption and not with proper Symmetric key



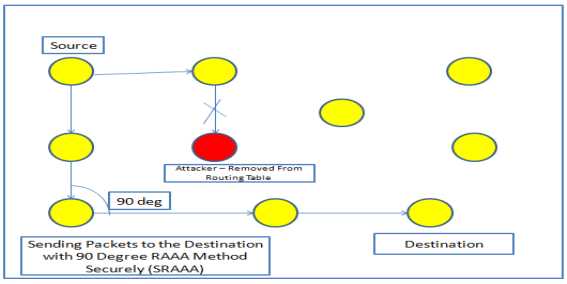
2.6: Otherwise append this host address to the route record, and rebroadcast this Request.
2.7: If this is the last RREQ retry, the node checks its eligibility to become a Smart node and send a SRREP to the source if it satisfies all the criteria
Step-3 Once Source receives the Reply from Destination, It will try to do MD5 Decryption to view the reply message



Step-4 Once it decrypted the message, it will assume the node is authenticated. If not able to decrypt, or symmetric key is not matched, it will immediately find that particular node is attacker.
Step-5 If the reply authenticated and found the attackers, source node start sending the Certificates to all the nodes which are authenticated



Step- 6 Nodes which are not authenticated or the nodes which are not having the certificate, it will get eliminate from the routing table
Step-7 RABGR process is started and nodes are finding distance and updating the Routing table with location.
Step-8 Finding Angle for all neighbor nodes and updating the routing table as per Biased routing of 90 degree right angle.
Step-9 If Source node receives SRREP then it store the smart route reply and wait for more reply. After the expiry the timer the source will select some of the Smart reply and send data to only those smart route.
Step-10 After getting data from the original source the intermediate node will do following
10.1- After receiving the data from the source, intermediate node will store the data and permanently checks for new locality.
10.2- When a intermediate node detect that it is in a new locality of 90 degree right angle node, it send a SRREQ to that particular node on behalf of the source.
10.3- If a next node will receive a Route Reply from the destination then it deliver its data to the destination .After delivering the data to the actual destination the intermediate node will send an acknowledgement to the actual source so that the source node will aware of this fact that its data is sent to the destination.
10.4- If intermediate node will not get a route Reply from the destination, there is link failure happened and activate multi path routing then Repeat Step 5(to select another intermediate node which keeps data on behalf of the previous intermediate node)
Step-11 if no nodes are found in 90 degree biased right angle, Ant search method will get activated and find the shortest path to the destination and update the routing table
Step-12 With the updated Routing table, the packets will go to the destination successfully



VIII. PERFORMANCE ANALYSIS

In this phase, the performance data of four routing protocols (TORA, ARIADNE, TESLA and SRAAA) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility pause time ranging from 0 to 100 seconds. The data is collected according to two metrics – Packet Delivery Fraction and Normalized Routing Load. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.

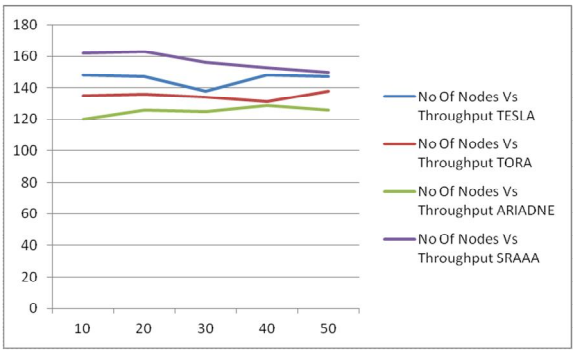


Fig. 7 Simulation Result of Node Vs Throughput

The Graph Shown in figure comprises the results of Throughput with no of node taking Throughput along Y-axis and No of node along X-axis. This graph shown in Figure indicates the throughput values for different number of nodes. We are comparing the developed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE.

The throughput outcome is good when compare with all other protocol. We obtained the transmission range of TX Range and the carrier-sensing range by similar approaches. We fixed the information table of each node and set the distance between successive nodes with the help of smart secured route using SRAAA.

SRAAA improves 11% of the throughput in terms of Number of nodes when compared with all other protocols.

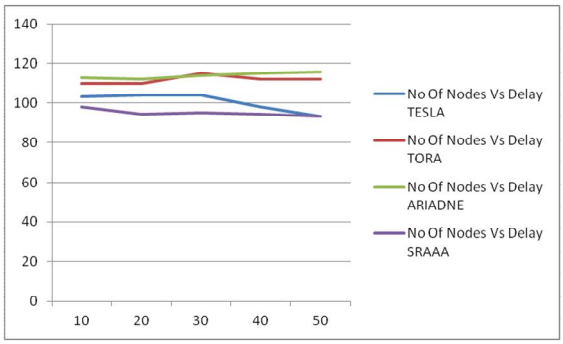


Fig. 8 Simulation Result of Node Vs Delay

The Graph Shown in figure comprises the results of delay with No of node, taking node along X-axis and Delay along Y-axis. Graph indicates the Delay values for different number of nodes.
We are comparing the developed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE. The Delay outcome is good when compare with all other protocol we measure the effect of change in number of nodes on packet delay. Each experiment is executed for 10ms. Delay from initial transmission of packet from source until packet is received at destination.

We can speculate that the reason is in the fact that small frame size results in larger number of frames, which in turn results in more dequeue attempts and more collisions and bakeoffs.

Smart secured route is used to reduce the delay with avoiding the waiting time Graph demonstrates the above point by measuring pure network delay (which excludes delay at the buffer). The buffer delay is the major factor in causing packet delay, while network delay is the minor factor. SRAAA improves 10.6% of the delay in terms of Number of nodes when compared with all other protocols.

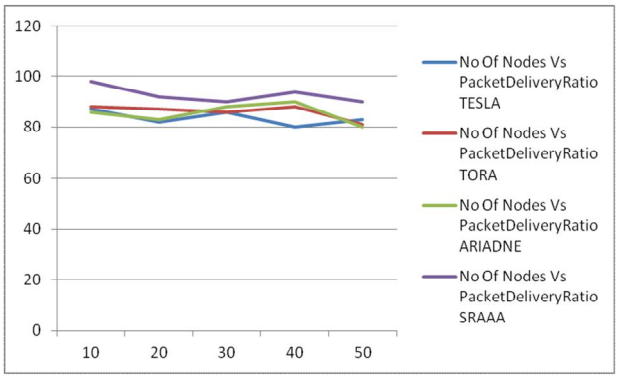


Fig. 9 Simulation Result of Node Vs Packet Delivery Ratio

The Graph Shown in figure comprises the results of Packet Delivery with No of node, taking node along X-axis and PDR along Y-axis This graph indicates the PDR values for different number of nodes. We are comparing the developed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE. The PDR outcome is good when compare with all other protocol. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes. Performance of the ARIADNE is reducing regularly while the PDR is increasing in the case of TORA and TELSA. SRAAA is better among the three protocols. SRAAA improves 9.5% of the Packet delivery ratio in terms of Number of nodes when compared with all other protocols.

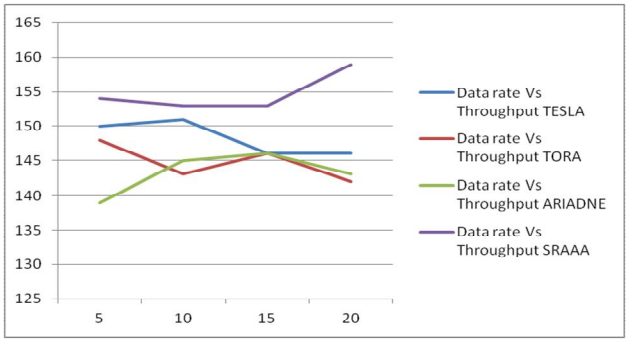


Fig. 10 Simulation Result of data rate Vs Throughput

Data rate defined as that number of packet sends per second. Here we are plotting the graph between Throughput and data rate. Data rate of a connection is a measure of how data bits can travel from one end to the other in a measurable amount of nodes. Throughput of a connection is a measure of how much information data can be moved from one end to the other in a measurable amount of time. The Graph Shown in figure comprises the results of Throughput with Data rate, taking data rate along X-axis and Throughput This graph shows that when the data rate is less, SRAAA throughput is better but as we increase the data rate from 5 to 20. RAAA improves 10.29% of the Throughput in terms of Data rate when compared with all other protocols

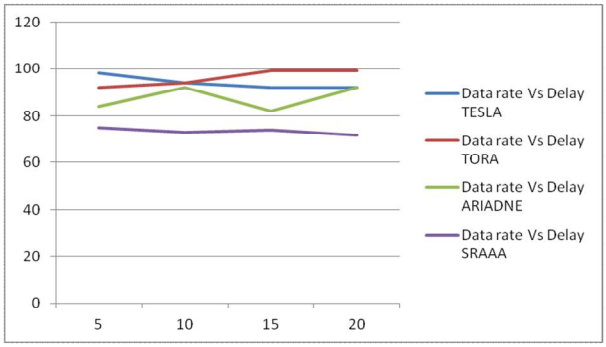


Fig. 11 Simulation Result of data rate Vs Delay

The Graph Shown in figure comprises the results of Delay with Data rate, taking data rate along X-axis and Delay along Y-axis, we could conclude that our SRAAA protocol has low delay at low data rate as well as at high data rate when compare to all other protocols. SRAAA improves 13.22% of the Delay in terms of Data rate when compared with all other protocols.

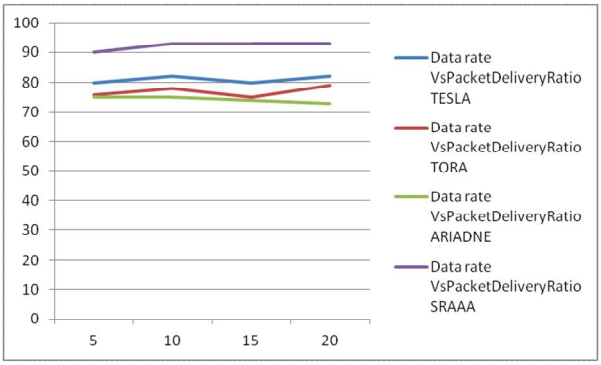


Fig. 12 Simulation Result of data rate Vs Packet Delivery ratio

The Graph Shown in figure comprises the results of Packet Delivery Ratio with Data rate, taking data rate along X-axis and PDR along Y-axis. This graph indicates that at low data rate the PDR of overall RAAA produce better Packet Delivery ratio as compare with others protocols. SRAAA improves 12.62% of the Packet delivery ratio in terms of Data rate when compared with all other protocols.

IX. CONCLUSION

This chapter has presented a secure routing protocol based on key management, a secure path and protecting data to satisfy our security requirements. After understanding security requirements and identifying the types of attack the network might face, we developed the security mechanism SRAAA most able to satisfy these security requirements, having the following elements:

1. SES encryption and Decription (used to protect non-mutable data)
2. MD5 Hash function (used to protect mutable data request)
3. Time synchronization.

All these mechanisms when applied to routing protocols should prevent external attacks, including black holes and routing holes, while providing viability, confidentiality and authentication. Time synchronization is used to provide the protocol with the ability to find the route and to ensure that the selected route is the correct path. The digital signature mechanism, when applied to routing protocols, should prevent internal attacks, including impersonation, and should provide non-reputation and integrity.

The solution is a combination of the history of the nodes and operation certificates. Each node in a secure environment is uniquely identified by its public key, Symmetric key and MAC address. The solution addresses various vulnerability issues affecting wireless links such as active and passive attacks. The dynamic nature of networks and their membership does not affect the solution, since each node makes access decisions on its own and the use of cooperative algorithms is avoided. We have compared RAAA with TORA, TESLA, ARAN, ARIADNE protocol and proved that our SRAAA is more better that all other protocols and increased the security level from 75% to 86%.

X. REFERENCES

[1] K. Thamizhmaran1, R. Santhosh Kumar Mahto, V. Sanjesh Kumar Tripathi, "*Performance Analysis of Secure Routing Protocols in MANET*", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012.

[2] Arvind Dhaka, raghuveer Singh Dhaka, priyank hada, "*A security in zone routing protocol for Manet*", IJREAS volume 2, issue 2 (February 2012).

[3] S. Nithya Rekha1, C. Chandrasekhar and R. Kaniezhil, "*Efficient Routing Algorithm for MANET using Grid FSR*", 2011 International Conference on Advancements in Information Technology.

[4] Gaurav kadyan, sitender malik, "*comparative study of various hybrid routing protocols for mobile adhoc network*", international journal of latest research in science and technology vol.1, issue 2: page no145-148, July-august 2012.

[5] K. Sahadevaiah, "*Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc networks*", Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 4, 2010.

[6] Priyanka Goyal1, MANET: Vulnerabilities, Challenges, Attacks, Application, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[7] Attila A. YAVUZ, Faith ALAGOZ, " *A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption*", Turk J Elec Eng & Comp Sci, Vol.18, No.1, 2010.

[8] Augustan Caminero," *Network-aware Peer-to-Peer Based Grid Inter-Domain Scheduling*", at 2008.

[9] Ramesh, D. and A. Krishnan, " *An Optimal Load Sharing Technique for Grid Computing*", American Journal of Applied Sciences.

[10] Ying Chen, Ataul Bari, "*Techniques for Designing Survivable Optical Grid Networks*", JOURNAL OF COMMUNICATIONS, VOL. 7, NO. 5, MAY 2012.

[11] Takeshi Matsuda, Hidehisa Nakayama," *Gateway Selection Protocol in Hybrid MANET Using DYMO Routing*", 2010.

[12] [S.Sriram, Sunther,"*Performance Evaluation of Route Securing Protocols in MANET*", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[13] Celia Li, Zhuang Wang, and Cungang Yang, "*Secure Routing for Wireless Mesh Networks*", International Journal of Network Security, Vol.13, No.2, PP.109–120, Sept. 2011.

[14] S. Prasad, Y.P.Singh, and C.S.Rai, "*Swarm Based Intelligent Routing for MANETs*", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[15] Parul Tomar, Prof. P.K. Suri, "*A Comparative Study for Secure Routing in MANET* ", International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010.

[16] A. M. Kamal, "*Adaptive Secure Routing in Ad Hoc Mobile Network*," M.S. Thesis, Dept. Computer and Systems Science, Royal Institute of Technology, Stockholm, Sweden, 2004.

[17] Z. J. Haas, M. R. Pearlman, P. Samer, "*The Zone Routing Protocol (ZRP) for Ad Hoc Networks*," Internet Draft, 2003, available at:http://tools.ietf.org/id/draft-ietf-MANETs-zone-zrp-04.txt.

[18] M. Poturalski, P. Papadimitratos, J. Hubaux, "*Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility*," in Proc. ACM Symposium on Information, Computer & Communication Security ASIACCS'08, Tokyo, Japan, 2008.

