SRIP: A New Way of Enhancing the Security of MANETs Using Secure Routing Information Protocol

[1]BalamuralikrishnaThati, [2]Dr.Mohammed Ali Hussain

[1]Research Scholar, Department of Computer Science, Bharathiar University
[2]Professor, Department of Electronic Computer Science & Engineering, KL University**

Abstract. **The study is purely related to the problem of enhancing and managing of security in a new way for Mobile Ad-hoc Network (MANET). The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploits the cooperative behavior of the ad-hoc routing. The main objective of this paper is to enhance the security against routing attacks in MANETs. Here the intrusion detection is based on Secure Hashing Algorithm 512 (SHA512) is implemented for the Authentication and Data Integrity of the information being sent Trust-Based system is formulated for preventing the Denial-of-Services (DoS) Attacks. The first part of this paper applied the SHA512 for ensuring that the data packets are received by the destination only and in its original form but at the expense of the increased processing time at the source and the destination. The second part uses the Trust-Based system with those nodes that act maliciously being broadcasted in the network and isolated to render a higher throughput and packet delivery fraction but at the expense of the increased end to end delay.**

Keywords**: MANET, Dual Authentication Hashing Technique (DAHT), Security, Routing Attacks, Trust Based System.**

1 Introduction

Regularly, Multicast based communication is a vital network service, which sends the data from a source to multiple destinations simultaneously by creating copies only when the links to the destinations split. Multicasting can reduce the cost of communication, consumption of bandwidth, sender and router processing and delivery delay.

An attention- grabbing and difficult issue of ad-hoc networks is its potential use in places wherever the infrastructure support to run a traditional network does not exist. Some applications embrace a compact zone, an isolated remote space, a disaster zone like earthquake affected region and virtual class room etc. In ad hoc networks all nodes are accountable of running the network services which means that each node cojointly works as a router to forward the networks packets to their destination. Providing security becomes even tougher when the collaborating nodes are mostly less powerful mobile devices.

A MANET with desired characteristics initially developed entirely for military purposes, as nodes are speckled over a battlefield and there is no specific infrastructure to help them to form a network. In the years that followed, MANETs were developed rapidly and have found increased usage in many applications, transforming from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or human interaction. Some examples are search and rescue missions, data collection, virtual classrooms and conferences where laptops, Personal Digital Assistant (PDA) or other mobile devices share wireless medium and communicate between each other. There are possibilities for the nodes in the network to be malicious or selfish. Therefore, even a single compromised node can lead to failure of the entire network.

2 RELATED RESEARCH

Dilli Ravilla and Chandra Shekar Reddy Putta proposed that the HMAC-SHA512 for ensuring that the data packets are received by the destination only and in its original form but at the expense of the increased processing time at the source and the destination and Trust-Based system with those nodes that act maliciously being broadcasted in the network and isolated to render a higher throughput and packet delivery fraction but at the expense of the increased end to end delay.

Amit Chopra and Dr. Rajneesh Kumar introduced a self-organized hash based secure routing scheme for multicast ad hoc networks. It uses group Diffie-Hellman method for key distribution. Route authentication and integrity, both are ensured by generating local flag codes and global hash values. In the case of any violation, route log is monitored to identify the malicious activities.

According to L. Raja, Dr. P. S. Periasamy, a secured routing mechanism called the Dual Authentication Hashing Technique is employed to protect the routing packets instead of digital signature. Here it is assumed that no two compromised nodes are colluding and are within two hops of each other. In the initialization phase, a common secret is distributed among the two hop node group through management of the local node group.

Dona George, L.Raja presented a security to routing attacks in MANETs. Here the intrusion detection is based on DAHT (Dual Authentication Hash Technique which is based on end to end communication between the source and the destination. This technique will provide good security with much less overhead and delay than the existing system to protect the routing information.

3 MODEL DESCRIPTION

In the proposed approach a security mechanism called Hashing Technique SHA512 is used to protect routing packets instead of digital signature used in the existing system. Under the valid assumption that no two compromised nodes are colluding and are within two hops of each other, we adopt the double Hash authentications, one of which is used to authenticate the received routing packets and the other is used to prevent the current nodes modify the routing information themselves. If the routing information is modified by some compromised node its neighboring nodes can detect this misbehavior immediately. In a next phase, common encryption technique is distributed to two hop node group through management of the local node group. So authentication, misbehaving nature and data security is achieved greatly.

RREQ packets are authenticated with two hash values which are used to check whether the received routing packet has been modified and to prevent the current node modifying the packet.

This cryptographic hash function takes as a message of arbitrary length as input and generates as output a 512-bit (32 byte) message called digest also termed as SHA512 [7] hash or checksum which is used to check data integrity.

Optimal path discovery from the broken link failure node, from the set of discovery nodes path created from source node via previous path node of failure node to the destination node.

$$Z = \int_1^n P + \int_1^{n-1} \lambda_1 \quad (1)$$

Where Z is optimal path discovery.
P is number of nodes.
λ 1 is previous node of link failure.
SHA-512 Hash computation processes message blocks M1, M2, … Mn. Using the Hash formulas

A1 = H[IDf , SN, Hc + 1 , M1, Ks], A2 = 0 ; Initially.

Then A2 is calculated as

A2 = H[IDf, SN, Hc, M1, Ks]. (2)

These two packets are sent through RREQ packets.
Where H is Hash function.
A1 is Hash value for one-hop group.
A2 is Hash value for two-hop group.
IDf is Identification of source node in the network.
SN is Sequence number of a packet over network.
Hc is Hop count which is distance between source and destination in an identified path in the network
M1is Original Message that is being transmitted over network.
Ks is Secret Key which is issued by the trusted system to all the nodes in the network.

In the route Hop count is < Advertising Hop count (3)

Encrypted data is E[H[IDf, SN, Hc+1, M1, Ks, ts], kp] (4)

Where E is Encryption algorithm and kp is public key and ts is time stamp value.

3.1 ALGORITHM FOR EVALUATING SRIP ALGORITHM

Step 1: By sending RREQ packets are transmitted to all the nodes in the n/w. First we find out secure route using MADAAOMDV. By getting RACK from all the destination nodes in the n/w.

Step 2: In order to know whether the Route is secure or not (any misbehaving nodes present in the n/w) we use dual hash technique A1, A2.
Here, to calculate hash value we use SHA512 with their hash values as follows
A1 = H[IDF, SN, HC-1, M, KX];, A2 = 0;
We send A1 and A2 values along with RREQ packets.
Likewise, RREQ packets are transmitted from 1-H TO 2-H are transmitted to n/w.
Here hash values are calculated using hop count.

Step 3: Generally every node maintains route table. So the first node can distribute advertizing Hop count value to 1-H group.

If alternate hop count < advertising hop count value then alternate hop count can be considered as new route. Based on that all the nodes in that route can modify their route table along with adjacent nodes and corresponding hop count and trust value.

Step 4: By using PKI we send local values and global values to all the nodes in the n/w.

Step 5: In order to provide total security to data RSA algorithm is used by encrypting the whole Transmission process.

4 Presentation Valuation of the Planned Algorithm

Here two security mechanisms i.e., Hashing Technique SHA512 and Encryption performance are verified and results are observed and presented. In this set of simulation 50 nodes are randomly deployed in flat space with a size of 800*800 m2. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. Transmission ranges of nodes is set to 200m. Here we consider three performance metrics.

Packet delivery ratio: PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

Throughput: is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

End-to-End Delay: End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from round-trip time (RTT) in that only path in the one direction from source to destination is measured.

Radios	Through put in kbps	Packet delivery fraction	e2e in ms
1	18.7	0.79	1460
2	186.7	0.89	930
3	91.1	0.80	990
4	87.5	0.80	860
5	62.6	0.80	970

Table.1. The performance parameters of the SRIP with SHA512-encription.

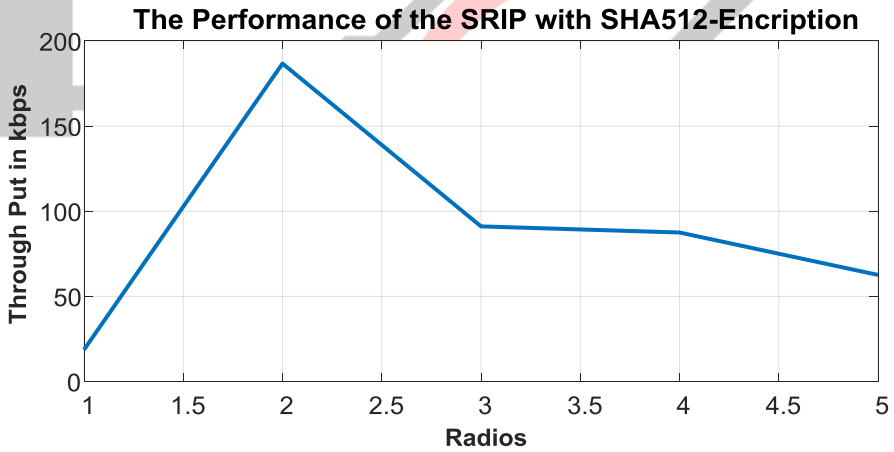

Figure.1. The performance of SRIP with SHA512-Encryption for Throughput.

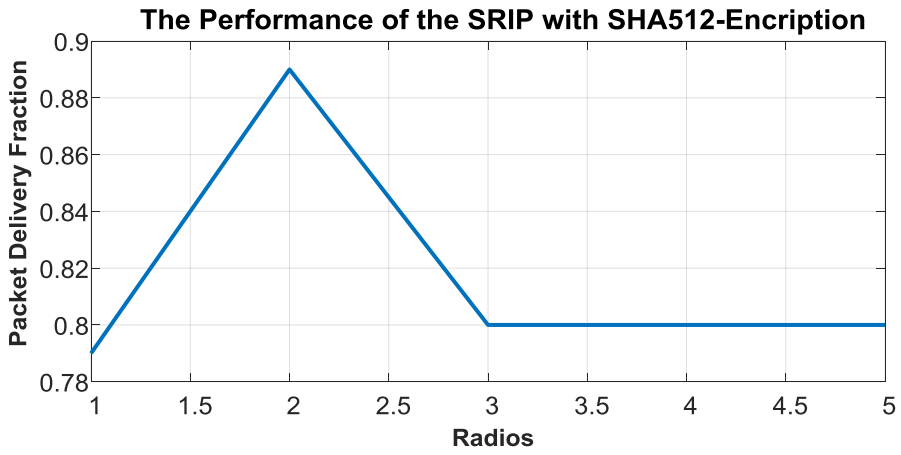

Figure.2. The performance of SRIP with SHA512-Encryption for Packet Delivery Fraction.

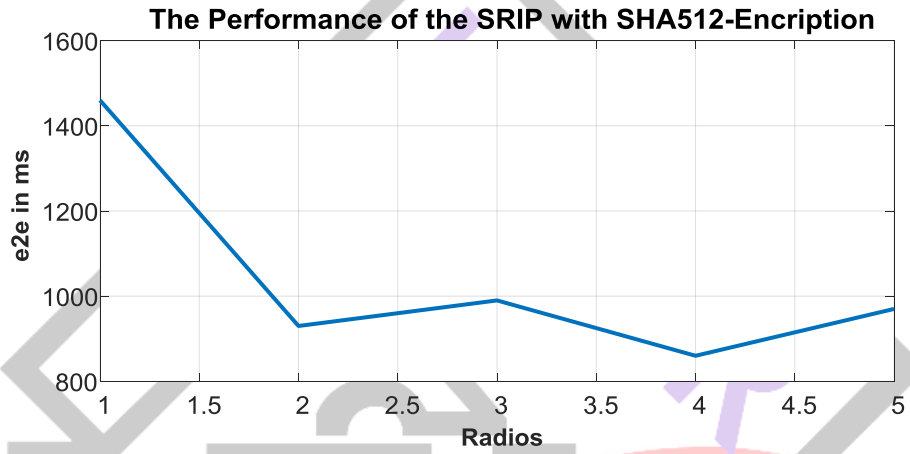

Figure.3. The Performance of the SRIP with SHA512-Encryption for End-to-End Delay.

The results of the advanced SRIP with SHA512 can be seen in Table 1. The performance parameters are Throughput, Packet Delivery Fraction and End-to-End Delay. Looking at the above Tables 1 we can conclude that at radius = 1, the protocol is reactive or demand driven and hence many hops are required to send the data to the destination that results in lower throughput and pdf but higher e2e delay. For radius from '2' to '5', we can see that the throughput is decreasing because the proactive approach gets predominant and has to fan out more and more nodes in the zone but this approach reduces the e2e delay and can be verified from the table.

MALC%	PDF
0	0.97
1	0.84
2	0.60
3	0.40
4	0.36
5	0.32

Table.2 Effect of malicious nodes

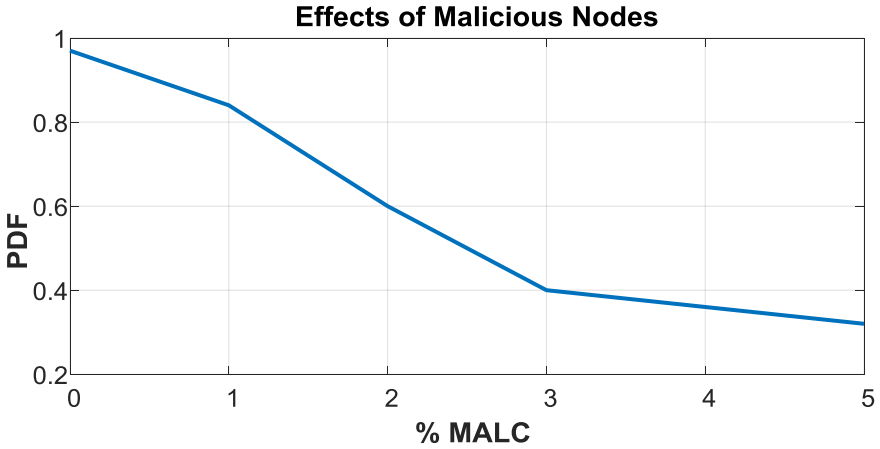

Figure.4. The effects of malicious node via PDF.

With the above parameters, the analysis is done and the Packet Delivery Fraction is evaluated as given in Table 2. From Table 2, we can conclude that when the malicious node percentage reaches around 30, there is a sharp decrease in the Packet Delivery Fraction. Thus, the tolerable limit of malicious node is less than 30% without having much of an effect on the performance of the network.

The following two scenarios are considered and taken print from NS-2 tool, one in the beginning of the network construction, another is after completion of the network simulation model.

Fig. 3. Before the operation of the simulation with an initial nodes 20, certain speed, and path time.

Fig. 4. After the operation of the simulation the position of nodes with calculation of link breakage.

5. CONCLUSION

In our work, the routing approach in mobile ad hoc networks with respect to the security is considered and analyzed the various threats against mixed routing in ad hoc networks and proposed the requirements which are essential to be addressed for secure routing. In this paper two techniques namely SHA512 and encryption for providing data integrity along with authentication and Trust-Based system to make the network more secure by preventing Denial of Service attacks in the network are used. Our proposed protocol reaches a better result towards accomplishing the security goals such as message integrity and message authentication, by taking a unique method called time stamp value. Along with cryptography based solutions, a Reliable solution is also developed which is based on the advertisement hop count of the nodes.

The first part of the paper is development of SHA512 which provides us data integrity and authentication. The other part being the implementation of the reliable method that considers the malicious nodes of the network and tries to avoid them as these nodes affects the Packet Delivery Frequency (PDF). The reliable method increases the PDF. The simulations further show that as the malicious nodes percentage goes past 30%, the performance of the system degrades considerably. Furthermore, the mobility plays an important role while analyzing the network. If the pause time is increased, the mobility decreases that leads to more stable networks .Therefore, SRIP is an efficient way of identifying and organizing routes in an open environment.

REFERENCES

[1] T. Balamuralikrishna, Dr. Md Ali Hussain : A Stochastic Analytical Model for Evaluating Routing Performance of AODV Protocol for MANETs in : International Journal of Advanced Research in Computer Science and Software Engineering, 2016 March ISSN: 2277 128X, Volume 6, Issue 3.

[2] T. Balamuralikrishna, Dr. Md Ali Hussain : Design and Development of an Efficient Routing Protocol for Mobile Ad hoc Networks in : International Journal of Emerging Engineering Research and Technology; 2015 April :Volume -3 , Issue – 4 (A).

[3] T. Schiex, H. Fargier, G. Verfaillie, Valued constraint satisfaction problems: hard and easy problems, in proceedings of IJCAI'95, Montréal, Canada.1995 march; 4(1), 4202-4212.

[4] V. Rishiwal, M. Yadav, S. Verma, Power aware routing to support real time traffic in mobile adhoc networks, in: Proceedings of 1st International Conference on Emerging Trends in Engineering and Technology. 2008 July; 1(1), 206-217.

[5] A. Nagy, A. El-Kadi, M. Mikhail, Swarm congestion and power aware routing protocol for manets, in: Proceedings of 6th Annual Communication Networks and Services Research Conference.2008 May; 6(3), 1802-1817.

[6] N. Brougham, Y. Song, A new routing metric for satisfying both energy and delay constraints in wireless sensor networks, Journal of Signal Processing Systems .2008 May ; 51 (2) , 137–143.

[7] M.Heni, R. Bouallegue, (2012), "Power Control in reactive routing protocol for mobile ad hocnetwork", International Journal of Wireless & Mobile Networks (IJWMN). 2012 February; 3(3), 220-232.

[8] AsisNasipuri, Kai Li and Uma Reddy SappidiPower Consumption and Throughput in Mobile AdHoc Networks using Directional Antennas TO APPEAR IN THE PROC. OF IEEE INTER. CONF. ON COMP. COMM. AND NETWORKING (IC3N'02) . 2002 November; 8(5), 331-342.

[9] Energy-aware routing algorithms for wireless ad hoc networkswithheterogeneous power supplies JavadVazifehdanComputer Networks. 2011 May; 55 (2), 3256– 3274.

[10] AbdellahIdrissi, HOW TO MINIMIZE THE ENERGY Saad.T.H. E.Fadil,"Queuing Approach to Estimate the MANET's Optimal Number of Nodes",Oriental Journal of Computer Science & Technology.2012; 5(2), 205-214.

[11] G.Madhavi, M.K.Kaushik., "Queuing Methodology Based Power Efficient Routing protocol for Reliable Data Communications in Manets", 2013; 4(1), 277-289.

[12] N.Bisnik, Alhussein A, Abouzeid, "Queuing network models for Delay analysis of multi hop wireless ad hoc networks", Adhoc Networks, Elsevier.2009 November ; 2(2), 79-97.

[13] Gaurav K., G.Prasanna, Ch.Hota, "Probabilistic Routing using Queuing Theory for MANETs", International Journal of Wireless & Mobile Networks.2011; 3(4), 144-158.

[14] K. Vinoth Kumar1 * and S. Bhavani"An Efficient Secured Localization based Optimized Energy Routing for MANET 2Indian Journal of Science and Technology". 2015 December; 8(35).

[15] A. Sumathi* and B. VinayagaSundaram "An ANN Approach in Ensuring CIA Triangle using an Energy based Secured Protocol E-AODV for Enhancing the Performance in MANETS "Indian Journal of Science and Technology. December 2015; 8(34),17485- IPL0821.

[16] Balamurugan1* and S. Applaud Alias Balamurugan2 "Performance Analysis of AD-HOC on-Demand Distance Vector Routing Protocol N. M. "Indian Journal of Science and Technology.2016.