Performance Analysis of SSA under the Secure Environment

Navpreet Bhathal[1],
M. Tech Student
Department of C.S.E
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India.

Sukhpreet Kaur[2]
[2]Assistant Professor,
Department of C.S.E
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India.

Abstract-A mobile impromptu network (MANET) may be a endlessly self-configuring, infrastructure-less network of mobile devices connected while not wires. Security in MANETs may be a pressing issue, that wants immediate analysis attention. during this analysis a routing protocol is updated victimisation the mix of RCRDB with Associate in Nursing coding theme referred to as AES. The sweetening of the independent agency routing protocol is completed by applying security on that. The protocol chosen for sweetening is RCRDB. By victimisation the RCRDB non-public key technique, we are able to cipher any size of file, furthermore as any quite file. However because it has excessive latency and cargo drawback. To beat the matter of latency and cargo within the network RCRDB is combined with AES. AES is predicated on a style principle called a substitution-permutation network, combination of each substitution and permutation, and is quick in each software package and hardware. victimisation the RCRDBAES rule the delay and cargo within the network. The validation of the approach for reduction within the delay and therefore the reduction in load is conferred in results and discussion.

Keywords- RCRDB,AES, SSA

1. INTRODUCTION

A mobile specific network (MANET) is also a continuously self-configuring, infrastructure-less network of mobile devices connected whereas not wires. Specific is Latin and implies that "for this purpose". Manet is liberal to move severally in any direction, and might therefore modification its links to different devices usually. each ought to forward traffic unrelated to its own use, and so be a router. it's wide utilised in military &amp; civilian applications, search and rescue, temporary networks in meeting rooms &amp; airports, industrial applications and even in personal area networks. Security is also a basic and predominate demand for an advertisement hoc network as a results of its intrinsic vulnerabilities therefore as for users to perform protected peer-to-peer communication over multi-hop wireless channel. reckoning on the appliance context, a user would possibly need varied security services like authentication, integrity, non-repudiation, Confidentiality, Key and Trust Management and access management. not like wired networks that have dedicated routers, Manet has infrastructure-free network where the MNs themselves perform basic network perform as a router and packet forwarding[1].

2. ROUTING PROTOCOLS IN MOBIE AD HOC NETWORK

A number of routing protocols are projected and enforced for Manet so as to reinforce the information measure utilization, higher throughputs, lesser overheads per packet, minimum consumption of energy et al. of these protocols have their own benefits and drawbacks beneath bound circumstances. Routing protocols will be classified into 3 groups: reactive, proactive and hybrid. this can be summarized within the following figure 1:

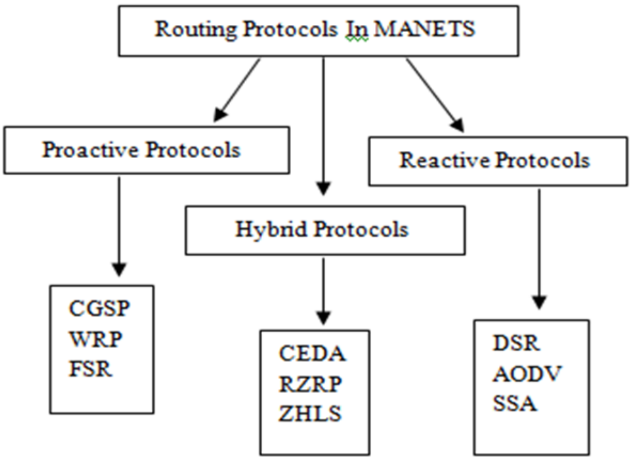

Fig 1: Classification of Routing Protocols

Pro-Active Routing Protocols

In table-driven or proactive protocols, the nodes maintain an energetic list of routes to every various node among the network throughout a routing table. The tables unit periodically updated by broadcasting knowledge to various nodes among the network just like the Destination Sequenced Distance Vector routing protocol (DSDV).[1]

Reactive Routing Protocols

In distinction to table driven routing protocols, on demand routing protocols notice route to a destination as long as it's required .The on-demand protocols have two phases in common – route discovery and route maintenance. among the route discovery procedure, a node want to talk with another node. The route maintenance section involves checking for broken links among the network and alter the routing tables. one all told the foremost common reactive protocols is impromptu on-demand Distance Vector routing protocol (AODV) [1].

Hybrid Routing Protocols

Hybrid routing protocols inherit the characteristics of every on-demand and table-driven routing protocols. Such protocols area unit designed to attenuate the management overhead of every proactive and reactive routing protocols [2].

3. Related Work

Shiv Prakash et al. [1] declared that Mobile sudden Network (MANET) is assortment of multi-hop wireless mobile nodes that communicate with each other whereas not centralized management or established infrastructure. The wireless links throughout this network square measure very error prone and should go down oftentimes thanks to quality of nodes, interference and fewer infrastructure. Therefore, routing in painter might be a vital task thanks to very dynamic atmosphere.

Ruchi Srivastava [4] declared that security is one in each of the biggest concern in MANETs as they are infrastructure-less and autonomous. Therefore, in painter networks in conjunction with security desires, there ought to be a pair of basic considerations unbroken in mind: foremost to make the routing protocol secure and second to protect the knowledge transmission.

Aarti and Tyagi S. S. [5] given the painter and its characteristics, challenges, advantages, application, security goals, varied types of security attacks in its routing protocols. Security attack can classified as a active or passive attacks. all totally different security mechanisms are introduced therefore on forestall such network.

Ramya K et al. [7] as long as to spice up the strength of the protection among the mobile adhoc networks, paper introduced academic degree innovative approach referred to as Hybrid Security Protocol that has integrity, confidentiality and authentication.

Hongbo Chou [8] declared that the elaborate study of routing protocols among the paper. ancient routing protocols are pictured among the paper and then painter protocols pictured for unicast, multicast and broadcast. Various protocols have different strengths and drawbacks. One protocol can’t match into all the potential eventualities and traffic patterns of painter applications. Hybrid unicast routing protocol appearance to be the next candidate than pure proactive and reactive routing protocols. However, its performance has got to be all exploited.

Deepthy J and Nishanth Krishnan [13] made public that Mobile sudden Networks ar infrastructure-less networks where each node acts as sender, receiver to boot as router for exchange of data. These nodes square measure generally steam-powered and often they die out before data transmission is complete. These networks square measure very dynamic thanks to node quality leading to frequent link breaks.

Laxmi V. et al.[16] as long as in painter there are many crucial issues like energy consumption, QoS, exposure to attacks, link stability etc. ar potential to be unreliable thanks to node quality.

Dr. Prerna Mahajan et al. [19] declared that network security has become a significant issue. secret writing has return up as a solution, and plays a significant role in data security system. foremost the knowledge that's to be transmitted from sender to receiver among the network ought to be encrypted exploitation the key writing rule out cryptography. Secondly, by exploitation cryptography technique the receiver can browse the primary data.

Vikas Deswal [20] studied that government agency protocol itself offers the construct of network reconfiguration to supply the network stability. The government agency protocol is capable to identify the broken link over the network. as a result of the broken link is thought, it finds the reconfigured path to perform the rerouting for network communication. throughout this analysis paper the projected model is to boot made public with modified government agency protocol to hunt out Reconfigured path.

Mrinmoy Gosh associate degreed Pranam Paul [21] as long as Cryptography could be a very important tool of data security through mathematical manipulation of data with associate degree incomprehensible format for unauthorized person. Here a replacement developed technique named, “Replacement of Cyclic Regeneration of Distinct Block (RCRDB)” is mentioned. At first, plain text is rotten into some blocks, having equal length. With facilitate of all distinct blocks, some distinct blocks square measure regenerated. the tactic square measure aiming to be continued up to a finite level of regeneration. Finally by transcription and replacement of all blocks in provide stream or plain text, target stream or encrypted text square measure aiming to be generated.

4. Proposed Work

SSA protocol focuses on obtaining the foremost stable routes through an ad hoc network. The protocol performs on demand route discovery supported signal strength and website stability. supported the signal strength, Social Security Administration detects weak and sturdy channels at intervals the network. SSA divided into two cooperative protocols: the Dynamic Routing Protocol (DRP) and also the Static Routing Protocol (SRP). DRP uses two tables: Signal Stability Table (SST) and Routing Table (RT). SST stores the signal strengths of the neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. These signal strengths unit of measurement recorded as weak or durable. DRP receives all the transmissions and, once method, it passes those to the SRP. SRP passes the packet to the nodes higher layer stack if it is the destination. with the exception of all the advantages of the Social Security Administration routing protocol it's having a downside that it can-not provide security or any quite cryptography to the packets at intervals the network. therefore exploitation this proposal the protection at intervals the range of cryptography is to be provided to the Social Security Administration.

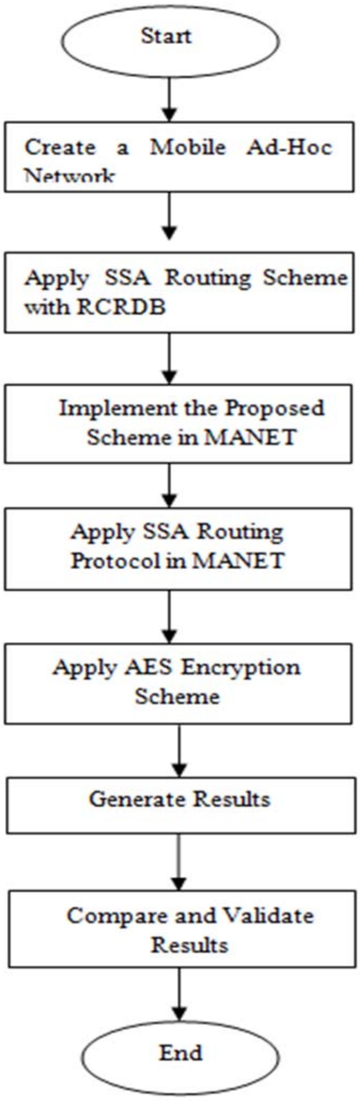
Start
Create a Mobile Ad-Hoc Network
Apply SSA Routing Scheme with RCRDB
Implement the Proposed Scheme in MANET
Apply SSA Routing Protocol in MANET
Apply AES Encryption Scheme
Generate Results
Compare and Validate Results
End

Figure 2: Flow chart for proposed scheme

5. Performance Parameters

There are different kind of parameters for the performance evaluation of the routing protocols. These have different behaviors of the overall network performance.These parameters are delay, load, througput, jitter, data dropped, packet delivery ratio, retransmission attempts for protocols evaluation.

Simulation Time: The time taken for each simulation to run or it can be said at the time between start and end of it.

Delay: Delay of network specified how long time takes for a bit/packet of data to travel across the network from one node to another.

Load: It refers to the amount of data that is carried by a network. It is expressed as bits/sec or packets/sec.

Throughput: It is an average rate of successful message delivery over a network. It is measured in Bits/sec or packets/sec.

Data Dropped: It is the amount of data that is not received to the destination and is dropped from the network. It is expressed in bits or packets.

Retransmission Attempts: It is the number of attempts that is taken by a source to deliver a message to the destination. It is represented in bits/sec.

Jitter: It is the total variation in the delay and transmission of packets from source to destination.

6. Simulation Experiments

OPNET is used as simulation tool for performance parameters. A scenario is set up for simulation to evaluate the performance of RCRDB and RDRDBAES. In OPNET Object oriented programming technique is used to create the mapping from the graphical design to the implementation of the real systems. So in this research, the comparison between RCRDB and RCRDBAES has been done using parameters load, jitter, throughput, delay. The results are as follows:

Figure 3 shows the pictorial view of jitter. Existing scheme possessed the delay which is 0.19 sec and that of in proposed scheme it is approx 0.12 sec. i.e. performance of proposed scheme is better than that of existing scheme.

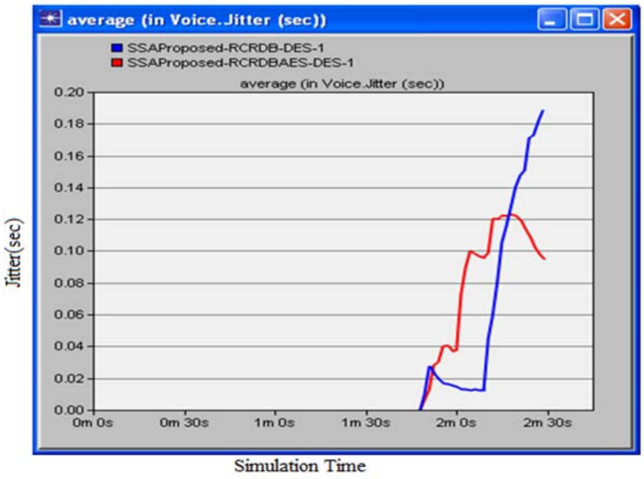

Figure 3: Jitter

Figure 4 shows the packet delivery ratio in case of base scheme is 0.8 packets but in case of proposed scheme it is approx 0.94 packets and proposed scheme has shown better result than base SSA routing scheme as packet delivery ratio should be more.

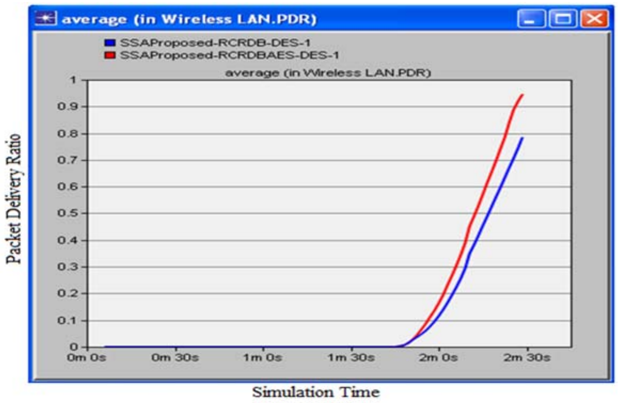

Figure 4: Packet Delivery Ratio

Figure 5 is the representation of load in existing and proposed SSA algorithm. Load in case of proposed algorithm is 5,000,000 bits/sec and that of existing scheme it is 9,000,000 bits/sec and proposed scheme has shown better result than existing SSA routing scheme. It depicts the less variation as compared to the base scheme.

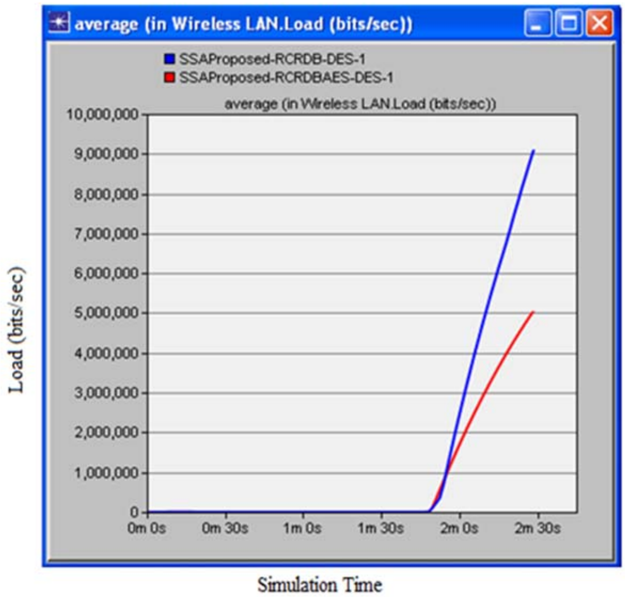

Figure 5: Load

Figure 6 shows the data dropped due to the Retry Threshold. Data dropped in case of base scheme is approx 65,000 bits/sec while in case of proposed scheme it is 67,000 bits/sec which shows that proposed scheme is approx equal as that of base scheme.

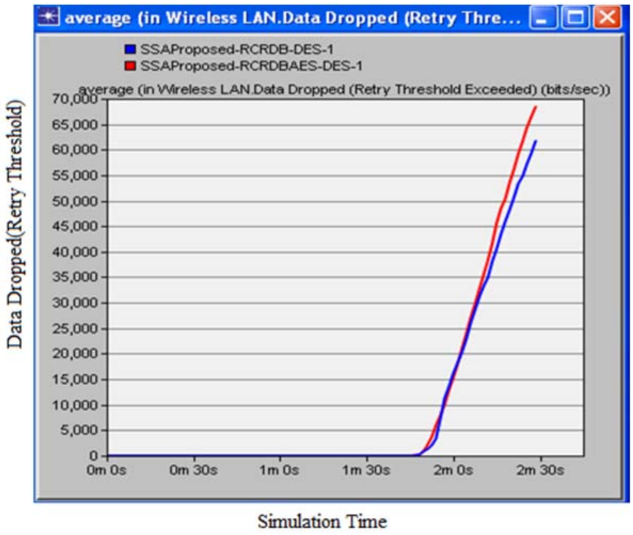

Figure 6:Data Dropped

This paper proposed comparison between RCRDB and combination of RCRDBAES. In the following table represented the comparative study of proposed and existing approach is done.

Table 1: Comparative study table of BSZRP and SZRP

Algorithm / Parameter	RCRDBAES	RCRDB
Packet Delivery Ratio	0.94	0.8
Load(bits/sec)	5,000,000	9,000,000
Jitter(sec)	0.12	0.19
Data Drop	8,800,000	4,800,000

7. CONCLUSION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANETS can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications. Signal Stability-Based Adaptive (SSA) Routing Protocol uses signal stability for finding stable routes. The signal strength is used to classify a link as stable or unstable. SSA detects weak and strong channels in the network based on the signal strength. But it has limitation of security. The enhancement of SSA is done by applying security on it. To provide security a combination of RCRDB and AES has been used. By using the RCRDB private key technique, we can encrypt any size of file, as well as any kind of file. AES is more secure and it supports larger key sizes than RCRDB. AES is faster in both hardware and software. So the combination of AES and RCRDB is used to provide the security to SSA. The results of the parameters load, delay, throughput, packet delivery ratio, jitter, retransmission attempts that are improved using a network simulator called OpNET. This problem is reduced in the proposed approach using combination of RCRDBAES encryption technique which makes little delay and low load in the network.

8. FUTURE SCOPE

In the future scope the data drop of the network can be reduced. In this work the combination of RCRDB algorithm and AES encryption scheme i.e. RCRDBAES encryption scheme is applied. The scalability of the approach can be improved so that quality parameters cannot be reduced.

REFERENCES

[1] Shiv Prakash, Rajeev Kumar, Brijesh Nayak, Manindar Kumar Yadav, "A Survey on Reactive Protocols for Mobile Ad Hoc Networks (MANET)," Proceedings of the 5th National Conference; INDIACom-2011, Computing For Nation Development, March 10–11, 2011, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.

[2] P.Srinivasan, K.Kamalakkannan, "Signal Strength and Energy Aware Reliable Route Discovery in Manet," International Journal of Communication Network Security ISSN: 2231–1882, Volume-1, Issue-4, 2012.

[3] Amol Bhosle, Yogadhar Pandey, "Applying Security to Data Using Symmetric Encryption in MANET," International Journal of Emerging Technology and Advanced Engineering, Volume-3, Issue-1, January 2013.

[4] Ruchi Srivastava, "A New Routing Algorithm With Security Considerations in Manet," International Journal of Communication and Computer Technologies, Volume- 01, No.61, Issue-7, August 2013, ISSN: 2278-9723.

[5] Aarti, Tyagi S. S., “Study of MANET: Characteristics, Challenges, Application and Security Attacks,’’ International Journal of Advanced Research in Computer Science and Software Engineering (CSSE), ISSN: 2277-128X, Volume-3, Page No. 252-257, May 2013.

[6] Lalit Kumar, Vikas Rana, Akash Rana, "An Algorithm for Secure Key Distribution and Data Transfer in Manet," International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3, Issue-4, April 2013, ISSN: 2277 128X.

[7] Ramya K, Beaulah David, Shaheen H., "Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET," OSR Journal of Computer Engineering (IOSR-JCE)e-ISSN:2278-0661, p-ISSN:2278-8727 Volume-16, Issue-1, Volume-8, February 2014, Page No.32-36.

[8] Hongbo Zhou, “A Survey on Routing Protocols in Manet”, Proc. of Michigan State University, MSU-CSE-03-08, March 2003.

[9] Nadia Qasim, Fatin Said, Hamid Aghvami, “Mobile Ad Hoc Networks Simulations Using Routing Protocols for Performance Comparisons,” Proc. of the World Congress on Engineering , Volume-1, WCE 2008, July 2008.

[10] Kuncha Sahadevaiah, Oruganti Bala, Venkata Ramanaiah, “An Empirical Examination of Routing Protocols in Mobile Ad Hoc Networks,” Proc. of International Journal of Communications, Network and System Sciences, June 2010.

[11] Parma Nand, Dr. S.C. Sharma, “Comparative Study and Performance Analysis of FSR, ZRP and AODV Routing Protocols for MANET,” Proc. of International Journal of Computer Applications (IJCA), 2011.

[12] Gaurav Kadyan, Sitender Malik, “Comparative Study of Various Hybrid Routing Protocols for Mobile Ad Hoc Network,” Proc. of International Journal of Latest Research in Science and Technology, ISSN:2278-5299 Volume-1,Issue -2, Page No.145-148, July-August 2012.

[13] Deepthy J, Nishanth Krishnan, "Performance Improvement of Energy Aware and Adaptive Routing Protocols for Manets a Survey," International Journal of Research in Engineering and Technology, e-ISSN: 2319-1163, p-ISSN: 2321-7308, Volume: 03, Special Issue: 01, NC-WiCOMET-2014.

[14] Ruchi Srivastava, "A New Routing Algorithm With Security Considerations in Manet," International Journal of Communication and Computer Technologies, Volume- 01, No.61, Issue-7, August 2013, ISSN: 2278-9723.

[15] Kavita Panday, Abishek Swaroop, “A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid MANETs Routing Protocols,” Proc. of International Journal of Computer Sciences Issues, volume-8, Issue-6, No. 3, Nov 2011.

[16] Laxmi V., Gaur M.S., Lal C., "LSMRP: Link Stability Based Multicast Routing Protocol in MANET,” IEEE Seventh International Conference Contemporary Computing (IC3), ISSN: 4799-5172, Volume-2 , Page No.254-259, Noida, 7-9 August 2014.

[17] Seon Yeong Han, Byoungheon Shin, Dongman Lee, "An Application-Driven Path Discovery Mechanism for Manet routing protocols,” IEEE International Conference Communications (ICC), ISSN: 0045-7906, Page No. 2822 – 2827, 14 June 2014.

[18] Gurvinder S.S., Vinay V., Rajesh K., "Comparing Popular Symmetric Key Algorithms Using Various Performance Metrics,” The International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Volume-1, Issue 7, December 2013.

[19] Prerna M., Abhishek S., "A Study of Encryption Algorithms AES, DES and RSA for Security,” Global Journal of Computer Science and Technology Network, Web & Security, ISSN: 0975-4350, Volume-13, Issue-15, version 1.0 Year 2013.

[20] Vikas Deswal, "Literature Survey of Network Reconstruction, Reconfiguration & QOS Optimization Approach in Case of Link Failure in Existing SSA Protocol in Mobile Ad-Hoc Network,” International Journal for Research in Applied Science and Engineering Technology, ISSN: 2321-9653.

[21] Mrinmoy G., Pranam P., "An Application to Ensure Security Through Bit Level Encryption," International Journal of Computer Science and Network Security, Volume- 9, No. 11, November 2011.