Mobile Ad hoc Networks using Secure Acknowledgements Techniques

Arulkumar M

Assistant Professor, Dept of Electronics and Communication Engineering,
Government College of Engineering, Bargur -635104

***Abstract*: A recent emerging research year the growing technology that allows to the users to access information and services anywhere regardless of their geographic location called as MANET. Mobile Ad hoc Network (MANET) is the significant technologies among various un-wired communication technologies where all the mobile nodes are mobile and which can be connected to random dynamically using wireless link in the random manner. It can provide Quality of Service (QoS) requirements in real update transmission for wireless application. But it stream including critical mission application like military use or emergency recovery. In this research paper proposed efficient Acknowledgements based Secure Quality Oriented Distributed, that cam improve a best performance of QoS with reducing delay also increase network communication throughput for Enhanced Adaptive 3 ACK's (S-EA3ACK) using EAACK (DSA) with MAJE4 symmetric cryptography specially designed for MANET through Network Simulator-2.34 (NS2) to implement it.**

***Keywords*: QOD, EAACK, S-EA3ACK, Cryptography, MAJE4.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 9, Issue 4, July-August 2021

1. Introduction

A dynamic Mobile Ad-hoc Network may be an assortment of all freelance mobile nodes with in active network which will communicate to every different mounted via radio waves. The mobile nodes that area unit in radio vary of every different will communicate directly, whereas others want the help of intermediate nodes to route their packets. Each node encompasses a through air interface to speak with different nodes. These networks area unit absolutely distributed, and may work anyplace while not the assistance of any mounted infrastructure as access points or base stations. Impromptu network area unit in the main subjected to 2 totally different levels of attacks. The primary level of attack happens on the fundamental mechanisms of the impromptu network love routing. Whereas the second level of attacks tries to break the safety mechanisms utilized within the network. Internal attacks area unit directly results in the attacks on nodes presents in network and links interface between them. This sort of attacks might broadcast wrong form of routing info to different nodes Internal attacks area unit typically tougher to handle as compare to external attacks, as a result of internal attacks happens due a lot of trusty nodes. The incorrect routing info generated by compromised nodes or malicious nodes area unit troublesome to spot. This will result to the compromised nodes area unit able to generate the valid signature mistreatment their non-public keys. These varieties of attacks attempt to cause congestion within the network, denial of services (DoS), and advertising wrong routing info etc. External attacks stop the network from traditional communication and manufacturing extra overhead to the

network. External attacks will classify into 2 categories: Quality of Service (QoS) refers to the aptitude of a network to supply higher service to choose network traffic over varied technologies, together with Frame Relay, Asynchronous Transfer Mode (ATM), LAN and 802.1 networks, SONET, and IP-routed networks that will use any or all of those underlying technologies. The first goal of QoS is to supply priority together with dedicated information measure, controlled interference and latency and improved loss characteristics. QoS technologies give the basic building blocks which will be used for future business applications in field, WAN and repair supplier networks.

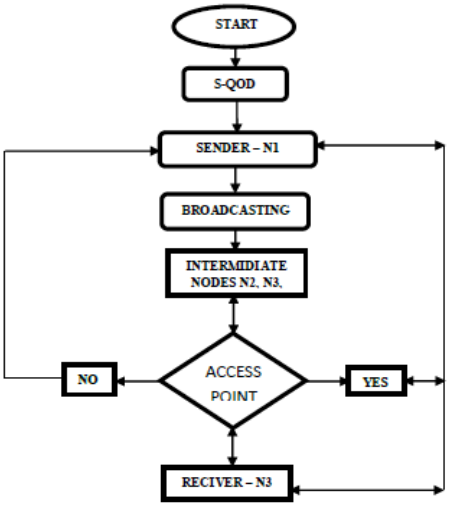
2. Methodology

In this paper, propose Secure Quality of Service orientated Distributed routing protocol (SQOD). Secure increased adjective three Acknowledgments (S-EA3ACK). Usually, Associate in Nursing on-demand network has widespread base stations. The info transmission in on-demand networks has 2 options. Associate in Nursing Access purpose (AP) may be a supply or a destination to any mobile node. Second, the amount of transmission hops between the mobile nodes Associate in Nursing an AP is tiny. After qualified neighbors are known, this algorithmic program schedules packet routing. A distributed queuing mechanism is given below. The supply node adaptively resizes every packet in its packet stream for every neighbor node in step with the neighbor's quality so as to extend the planning practicability of the packets from the supply node.

- The supply node adaptively resizes every packet in its packet stream for every neighbor node in step with the neighbor's quality
- The quality of a node will increase, the scale of a packet Sp sent from a node to its neighbor nodes i decreases as following :
- γ : Scaling parameter AN
- υi: The relative quality speed of the supply node and intermediate node =1 kb

Due to the broadcasting feature of the wireless networks, the APs and mobile nodes will catch and cache packets. Use AN end-to-end traffic redundancy elimination (TRE) rule eliminates the redundant information to enhance the QoS of the packet transmission. Specifically, higher than the algorithms employed in S-QOD, if a supply node isn't inside the transmission vary of the AP, a supply node selects near neighbors that may offer QoS services to forward its packets to base stations during a distributed manner show in figure 1 Data transmission of S-QOD. The supply node schedules the packet streams to neighbors supported their queuing condition, channel condition, and quality, reaching to cut back TRM and increase network capability. If any intermediate node cannot send the packets to destination. Check the node if it's affected from any wrongdoer or malicious used Secure increased adaptive three Acknowledgment (S-EA3ACK) theme.

Figure 1 S-QOD Data transmission

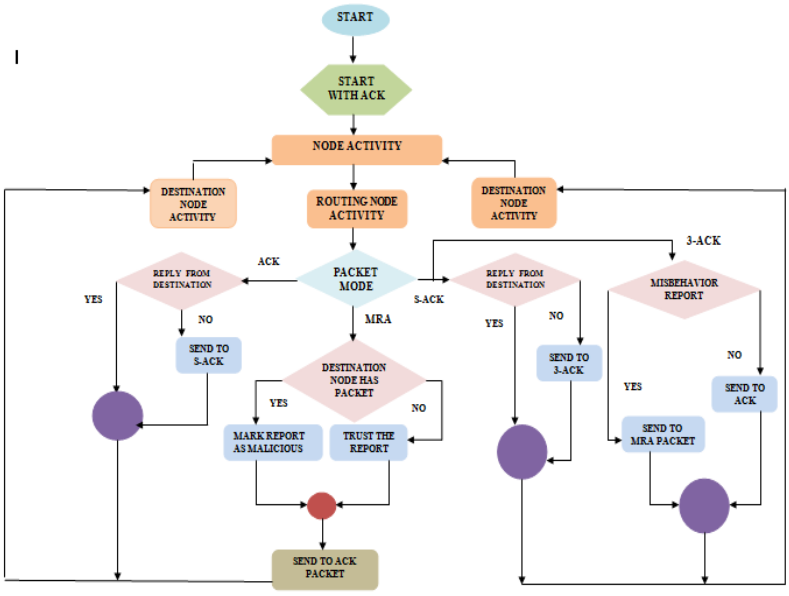


MAJE4

- Encryption for a protracted amount.
- Uses solely primitive procedure operations.
- Suitable for hand-held sort devices with restricted memory.

Use of quite one arithmetic and / or mathematician operator complicates scientific discipline. The secured selection is with the key sizes of 128 or 256 bits. To better investigate the performance of S-EA3ACK during this analysis work, it's accustomed check the new IDS's performance once the attackers square measure good enough to acknowledge packets and claim positive result whereas, in fact, it's negative. As Watchdog could be a un-acknowledgment-based theme, it's not eligible for this work a coffee level basic packet dropping attack is simulated the aim of this kind is to check the performance of IDSs against four weaknesses of Watchdog, namely, false wrongdoing, receiver collision, cooperative and restricted transmission power.

Figure 2 Flow diagram of S-EA3ACK



In this section, the projected S-EA3ACK theme is delineating thoroughly. The approach delineate during this analysis paper is predicated on the previous work (Shakshuki et al 2013), wherever the backbone of S-EA3ACK was projected and evaluated through implementation. It's extended with the introduction of MAJE4 cryptography to forestall the assailant from formation acknowledgment packets. S-EA3ACK consists of 4 major components, namely, ACK, secure ACK (S-ACK), 3-ACK and misdeed report authentication (MRA) so as to {differentiate} to tell apart} different packets in numerous forms of schemes In S-EA3ACK, three b of the various forms of packets is employed as show in figure 2 is flow diagram of EA3ACK. Details area unit listed in Table one and Figure a pair of that gift describing the S-EA3ACK theme. Please note that, within the projected effective secure theme, it's assumed that the link between each node within the network is full duplex diphase. What is more, for every communication method, each the transmitted node and also the receiver node aren't malicious, unless all acknowledgment and message packets delineate during this analysis area unit needed to possess same keys for the sender and receiver as show in table 1 packet type indicators.

Table 1 Packet Type Indicators

Packet type	General Data	ACK	S-ACK	3-ACK	MAR
Packet flag	00001	00010	00100	01000	10000

When comparing the simulation results with other research works, it is clear that the default scenario setting in NS 2.34 has been adopted. The maximum hops allowed in this configuration setting as show in table 2 simulation parameters.

Table 2 Simulation parameter

Parameter	**Value**
Simulation area	700 m * 700 m
Number of nodes	50
Average speed of nodes	0–20 meter/second
Mobility model	Random waypoint
Number of packet per/sec	4
Transmission range	300 m
Constant bit rate	3 (packets/second)
Packet size	512 bytes
Node beacon interval	0.5 (seconds)
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	600 sec
Malicious nodes	10

3. Result and Discussion

In this work, when the attackers are smart enough to acknowledge packets and claim positive result while, in fact, it is negative. Below table shows the simulation results that are based on different parameters.

Table 3 Simulation Result

Packet Delivery Ratio					
PDR / MN	10%	20%	30%	40%	50%
EAACK (S-QOD)	0.58	0.54	0.50	0.46	0.42
EA3ACK (S-QOD)	0.63	0.59	0.55	0.51	0.47
Throughput					
Throughput / MN	10%	20%	30%	40%	50%
EAACK (S-QOD)	0.33	0.43	0.42	0.48	0.51
EA3ACK (S-QOD)	0.24	0.30	0.39	0.38	0.41
Packet Loss					
Packet loss / MN	10%	20%	30%	40%	50%
EAACK (S-QOD)	0.03	0.035	0.04	0.05	0.06
EA3ACK (S-QOD)	0.02	0.01	0.015	0.02	0.03

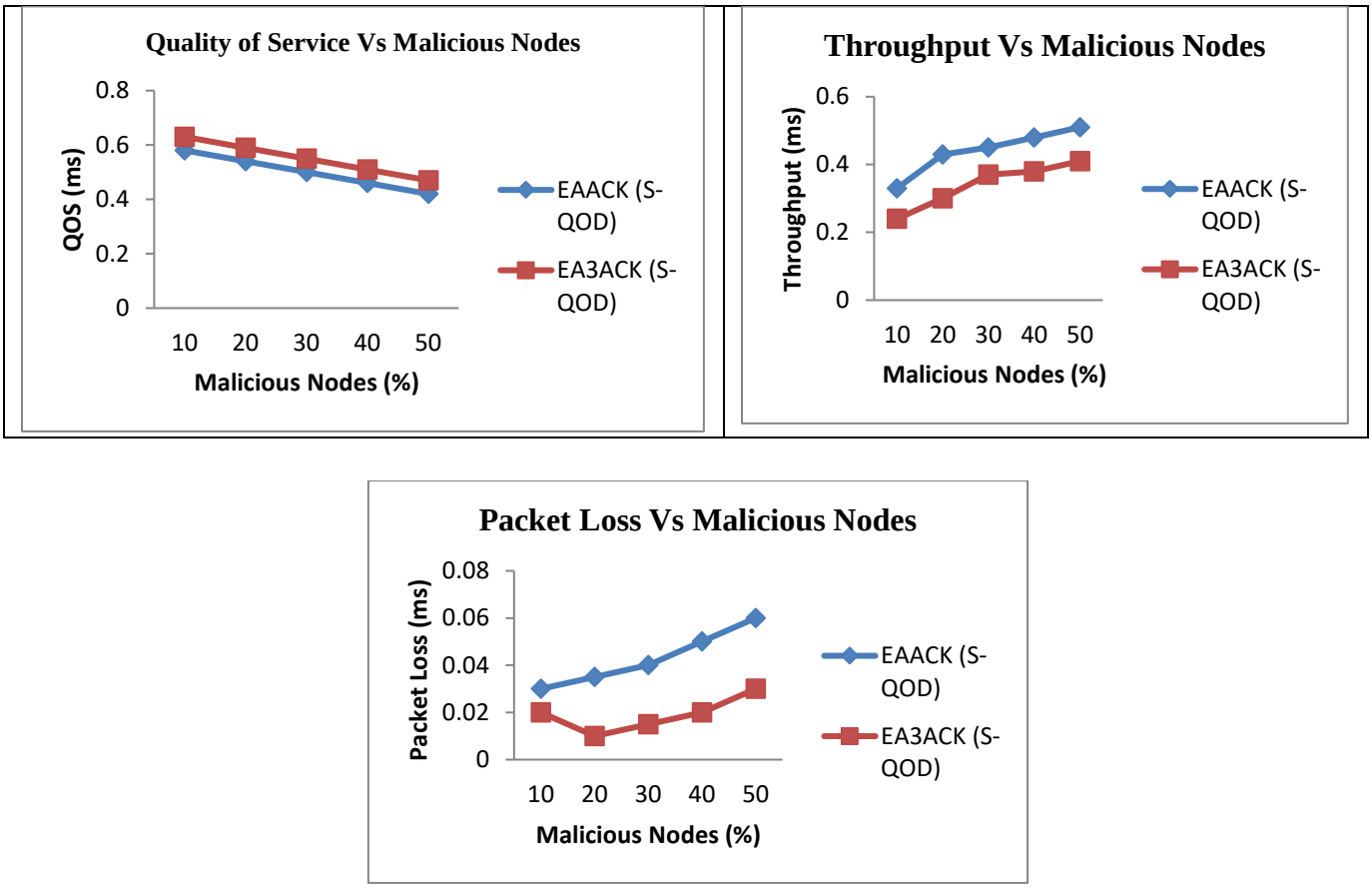


Figure 3 Packet Delivery Ratios, Packet Loss and Quality of Service Vs Malicious Node

From above Figure and Table it's clear that our proposed scheme S-EA3ACK surpassed EAACK performance by above 47% when there are 10% and 50% of malicious nodes in the network. S-EA3ACK (S-QOD) is able to detect misbehaviors in the presence of false misbehaver, receiver collision, limited transmission power and partial dropping. Comparing of the EAACK (S-QOD) with corresponding DSA algorithm with S-EA3ACK (S-QOD) shows the throughput increased with increase in the number of malicious nodes by 20% and 50%. Comparison of EAACK with corresponding S-QOD algorithm along with S-EA3ACK (S-QOD) where it shows the Packet loss ratio deceases with increase in the number of malicious nodes on by 10% and 50%. From all the higher than figures and table it's clear that the comparison of the S-

EA3ACK corresponding S-QOD algorithmic rule with EAACK with MAJE4 cryptography shows the turnout and packet delivery magnitude relation increase with the rise within the range of malicious nodes and additionally packet ratio decease with the rise within the range of malicious nodes.

4. Conclusion

Packet-dropping and loss attack have forever been a significant threat to the protection in MANETs. During this analysis paper, a completely unique IDS approach named S-EA3ACK protocol specially designed for MANETs is projected compared with alternative widespread techniques through simulations. Simulation results achieve positive performance of the delivery ratio, packet loss and quality of network S-EA3ACK (S-QOD) than EAACK (S-QOD) within the cases of receiver collision, restricted transmission power, false misbehavior report and cooperative attacks. Moreover, in an attempt to stop the attackers from initiating cast acknowledgment attacks, the analysis was extended to include Secure Quality destined Distributed during this paper. Improve secure transmission packet delivery quantitative relation with quality output and scale back packet ratio compared to the present EAACK (S-QOD) routing protocol. Each MAJE4 Cryptography and S-QOD schemes were implement through network machine two, the proposed algorithms is simulated in ns-2. We plan to develop the following future research work:

- ❖ It is core issues of secure and power aware/energy efficient routing.
- ❖ Use above following research work to develop energy efficient models use cluster network.
- ❖ We test some network model in real time environments.

There is no funding source for this research article

ACKNOWLEDGMENT

We would like to thank above researchers and respected internal expected reviewers who give their valuable review comments with suggestions for updating to improve quality of the paper. We would like to thank authorities of the estimated Government College of Engineering, Bargur, Tamilnadu, India.

REFERENCES

1 Shakshuki, et al. “EAACK - A Secure Intrusion Detection System for MANETs”, IEEE Trans.,2013, Vol. 60, No. 3, pp.1089-1098. https://doi.org/10.1109/TIE.2012.2196010

2 Prabu, K. and Subramani, A. “Energy efficient routing in MANET through edge node selection using ESPR algorithm”, Int. J. Mobile Network Design and Innovation, 2014, Vol. 5, No. 3, pp.166–175. https://doi.org/10.1504/IJMNDI.2014.065747

3 Thamizhmaran, R. Santosh Kumar Mahto, and V. Sanjesh Kumar Tripathi, "Performance Analysis of Secure Routing Protocols in MANET," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 9, pp. 651-654, November 2012.

4 Venkanna and Leela Velusamy, “TEA-CBRP: Distributed cluster head election in MANET by using AHP”, peer-to-peer Network Application, Vol. 9, 2016, pp. 159-170. https://doi.org/10.1007/s12083-014-0320-0

5 K.Thamizhmaran., M. Anitha and Alamelunachippan “Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm”, International Journal of Mobile Network Design and Innovation, Vol. 7, No. 2, pp. 88-100, 2017. https://doi.org/10.1504/IJMNDI.2017.085743

6 K. Thamizhmaran, M. Anitha and Alamelunachippan “Reduced End-To-End Delay for Manets using SHSP-EA3ACK Algorithm”, I-Manager Journal on Communication Engineering and Systems, Vol. 7, No. 3, pp. 9-15, 2018. https://doi.org/10.26634/jcs.7.3.14309
7 Thamizhmaran Krishnamoorthy, Akshaya Devi Arivazhagan, "Energy Efficient Routing Protocol with Ad hoc On-demand Distance Vector for MANET", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (lSCO) 2015.
8 Akshaya Devi Arivazhagan, et.al “Co-operative analysis of Proactive and Reactive Protocols Using Dijkstra's Algorithm” IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.
9 Vennila, K., and K. Thamizhmaran. 2017. Implementation of multilevel thresholding on image using firefly algorithm. International Journal of Advanced Research in Computer Science 8 (3):373–78
10 Akshayadevi Arivazhagan, et.al (2015) “Performance Comparison of on Demand Routing Protocols under Back whole For MANET”, Advance Research in Computer science and software Engineering, Vol. 5, No. 3, pp. 407 – 411.
11 K. Thamizhmaran (2016) “Performance Evaluation of EA3ACK in different topology’s Using EAACK for MANET, I - Manager Journal of information technology , Vol. 5, No. 4, pp. 5-10.
12 K.Thamizhmaran, M.Anitha and Alamelunachippan (2017) “Comparison and Parameter Adjustment of Topology Based (S-EA3ACK) for MANETs”, International Journal of Control Theory and Application, Vol. 10, No. 30, pp. 423-436.