Moderate Delay using Shortest Path based Acknowledgements Algorithm for MANET

[*]K. Thamizhmaran, [#]G.Girishkumar

[*]*Dept. of ECE, GCE Bodinayakkanur,* [#]*Dept. of EEE, GPTC Keezhapaluver,*
[*]*Theni, Tamilnadu, India – 625582,* [#]*Ariyalur, Tamilnadu, India – 621707*

Abstract: *The problem of finding the optimal path between two nodes is a well-known problem in network analysis. Optimal routing has been widely studied for interconnection networks this thesis work considers the problem of finding the best and minimum link breakage path. This chapter describes the secure hybrid shortest path (SHSP) for MANET to overcome the drawbacks of previous work (average delay) for MANET of the research done in this area. This research aims to propose secure hybrid shortest path - Enhance Adaptive 3 Acknowledgements (SHSP-EA3ACK) using EA3ACK algorithm. The main aim of the proposed research SHSP-EA3ACK algorithm is to reduce end-to-end delay and routing overhead with the number of malicious node detection during the communication through acknowledgement base.*

I. INTRODUCTION

In this research, the shortest path routing problem which belongs to the topological routing is investigated. This shortest path routing problem aims to find the shortest route from a source node to a destination node in a given network while minimizing the total cost associated with the path. The shortest path routing problem is a classical combinational optimization problem arising in many designs and planning contexts. There are several deterministic search algorithms for the shortest path problem: Dijkstra algorithm, Breadth-First Search algorithm, and Bellman–Ford algorithm etc. All these algorithms have a polynomial time complexity and are effective in the fixed infrastructure wireless or wired networks. But they exhibit an unacceptable high computational complexity for real-time communications involving rapidly changing network topologies. Therefore, the Dynamic Shortest Path Routing Problem (DSPRP) in a changing network environment (infrastructureless) has become an interesting topic in the recent years.

Shortest Path Algorithm

There are two basic shortest path algorithms available: Bellman Ford algorithm and Dijkstra algorithm. One of them can be used to solve the routing problem. The performance is based on the following steps:

- Each node calculates the distance between itself and all other nodes within the network and stores this information in the routing table.
- Each node sends its table to all the neighbouring nodes.
- When a node receives distance tables from its neighbours, it can calculate the shortest routes to all the other nodes and updates its own routing table to reflect any changes. Destination Sequenced Distance Vector (DSDV) routing protocol has been developed for ad hoc network. It is based upon the distributed Bellman-Ford Algorithm.

Shortest path routing algorithm selects a path on minimum cost to forward the data to the next node. This shortest path selection is done on the basis of different parameters like transmission cost which is calculated on the basis of routing table information, link stability factor and power consumption factor. The performance of the network is enhanced through shortest path routing, but it also depends upon the functionality of the routing protocol and the parameters selected for the shortest path routing.

II. PROBLEM DEFINITION

The dynamic nature of MANET requires the routing protocol to refresh the routing tables frequently and suffer from transmission time delay and congestion with packet dropping that are the results of the broadcasting nature of radio transmission since a node in MANET cannot directly communicate with the nodes outside its communication range, a packet may have to be routed through intermediate nodes to reach the destination. Hence, it becomes essential to monitor the constraints in intermediate nodes. Consequently, an efficient routing approach may generate route delay, packet dropping and route failures. The simplest scheme routing in MANET is the one to find a route without malicious nodes in the shortest path. In this methodology the aim is to provide unbreakable route to secure transmission with the shortest path. So a new routing algorithm named secure hybrid shortest path with enhanced adaptive 3 acknowledgement using EA3ACK with secure hybrid shortest path is proposed. This SHSP-EA3ACK provides better performance than the existing EAACK, and also reduces routing delay and packet dropping without any misbehaviour at intermediate nodes.

III. EXISTING CONCEPT

ACK

In 3-ACK mode, the four consecutive nodes (i.e., A, B, C, and X) work in a group to detect misbehaving nodes in the network. Node 'A' first sends out 3-ACK data packet P1 to node B. Then, node B forwards this packet to node C, node C forwards this packet to node X. When node X receives P1, and as it is the fourth node in this four-node group, fourth node is required to send back ACK acknowledgement packet to the node A through node B and Node C. If node A does not receive this acknowledgement packet within a predefined time period, all nodes B, C and X are reported as malicious.

IV. NEW PROPOSED CONCEPT

Hybrid Shortest Path Routing

The average conditional intermeeting time is used as link costs rather than the standard intermeeting time and the messages are routed over the network. A comparison is made between Hybrid Shortest Path Routing (HSPR) protocol and the existing system model based routing protocol through real trace driven simulations. The results demonstrate that HSPR achieves higher delivery rate and lower end-to-end delay when compared to the shortest path based routing protocols. This shows how well the conditional interconnecting time represents internodes link costs and helps in making effective forwarding decisions while routing a message. Routing algorithms utilize a model called store carry and forward, it generates the multiple messages from a random source node to a random destination node at every second.

Algorithm for Hybrid Shortest Path Routing in MANETs

Assumption: S-Source Node, D-Destination Node, Q-Queue, T-Traffic,

SN_i - Security level of Node i.

SP - Security level in the RREQ Packet {The Destination node sends RREP back}

Step 1: Send hello message (RREQ) from source to all other neighbour nodes.

Step 2: All the neighbours send the same message until destination is reached.

Step 3: Calculate its security level using secure routing for the following condition,

If (SN_i> SP) then, update the security level in the RREQ packet.

Else, broadcast the RREQ to its neighbor nodes.

Step 4: if network = T then

Node follows Q until reach the D.

Else HSPR → D {Hybrid Shortest Path Routing model}

Step 5: If network ≠ T then

HSPR → D

Else selected path drop the packets due to link breakage and find the alternate route to the D.

Step 6: All linked networks execute the same process using HSPR algorithm until D is reached.

The data are sent by wireless mobile network from the source to destination on this network topology. The source node collects the neighbor node list and transmits the data to destination intermediate network through the network. It gathers the data sending and receives process on the network and the traffic conditions to be checked on this access model. In this research network the data transmission time occurred traffic on the network, selects the alternate shortest path route to send the data and also the main shortest path routing in its function on the network. It is the more secured method because it reduces the packet delay and number of loss packets in the wireless MANET. Here, to use a hybrid proactive and then reactive model on the network performance is more secure for route request and route reply. The packet loss at a time is not equal to the loss when a more efficient and secure modeling method is used on routing problem on the system. When data are sent from the source to destination, the network finds the shortest path to check and then sends the data through the alternative path to the destination.

V. METHODOLOGY OF SHSP-EA3ACK

SHSP-EA3ACK consists of five major parts, namely, ACK, S-ACK, 3-ACK, MRA and secure hybrid shortest path. The introduction of hybrid shortest path cryptography algorithm in EA3ACK prevents the attacker from forging acknowledgement packets. In order to distinguish different packet types in different schemes of SHSP-EA3ACK, 3 bit binary (3b) packets are used. The details are listed in Table 1. To investigate the performance of SHSP-EA3ACK, the following simulations have been carried out.

Table 1 Packet Type Indicators

Packet type	General Data	ACK	S-ACK	3-ACK	MAR
Packet flag	001	010	011	100	101

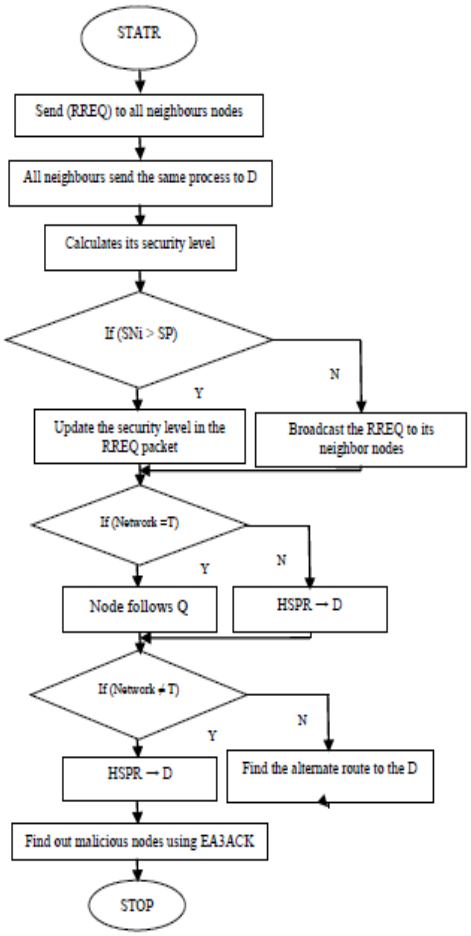

Fig. 1 Flow Diagram for SHSP-EA3ACK

Simulation configuration

The simulator NS-2.34 is used to test the intrusion detection systems performance when the attackers are smart enough to forge acknowledgement packets claiming positive result while, in fact, it is negative. As watchdog is not an acknowledgement based scheme, and as shown in Table 2, the following are the simulation parameters used for the analysis of routing protocol with hybrid shortest path algorithm.

Table 2 Simulation Parameters

Parameters	Values
Protocol	SHSP-EA3ACK
Simulation area	1,000 m * 1,000 m
Number of nodes	60
Average speed of nodes	0–25 meter/second
Mobility model	Random waypoint
Number of packet senders	40
Transmission range	250 m
Constant bit rate	2 (packets/second)
Packet size	512 bytes
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	500 sec

VI. PERFORMANCE EVALUATION

In this work, the malicious nodes are provided the ability to forge acknowledgment packets. This way, the malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to their previous nodes whenever necessary. This is a common method for attackers to degrade network performance while still maintaining their reputation.The proposed approach SHSP-EA3ACK is designed to tackle four of the six weaknesses of watchdog scheme, namely, receiver collision, limited transmission power, false misbehaviour and partial dropping.

The end-to-end delay performance of the proposed SHSP-EA3ACK and existing EAACK (DSA) protocol are compared.SHSP-EA3ACK has reduced end-to-end delay with the number of nodes increasedcompared to the existing EAACK (DSA) protocol. According to Fig. 2 and Table 3, the proposed scheme SHSP-EA3ACK surpasses the performance of EAACK (DSA) in minimizing average end-to-end delay by 21.4%, when there are 10 to 60 nodes in the network. As the proposed algorithm finds different short routes frequently, it is possible to minimize the delay.

Table 3 End-to-End Delay Vs. Number of Nodes

End-to-End Delay						
Routing / Number of Nodes	**10**	**20**	**30**	**40**	**50**	**60**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.57	0.52	0.47	0.41	0.33	0.24
SHSP-EA3ACK	0.48	0.44	0.39	0.31	0.24	0.17

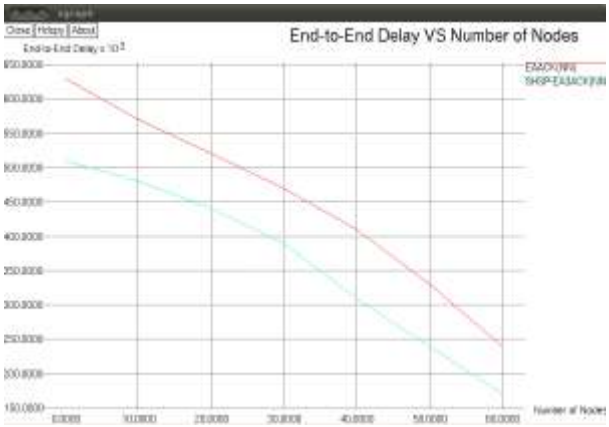

Fig.2 End-to-End Delay Vs. Number of Nodes

The end-to-end delay performance comparison of the proposed SHSP-EA3ACK and the existing EAACK (DSA) is show in Fig. 3 and Table 4. It is observed from Fig.3 that when compared with the existing EAACK (DSA) algorithm, the proposed SHSP-EA3ACK decreases the average delay by 23.5% with the increase in the number of malicious nodes from 3 to 18 out of 60 nodes. If the malicious node is detected, immediately the SHSP-EA3ACK algorithm finds alternate shortest route between the sender and receiver.

Table 4 End-to-End Delay Vs. Malicious Nodes

Malicious Nodes						
Routing / Malicious Node	**3**	**6**	**9**	**12**	**15**	**18**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.33	0.36	0.40	0.44	0.45	0.47
SHSP-EA3ACK	0.23	0.27	0.32	0.34	0.35	0.37

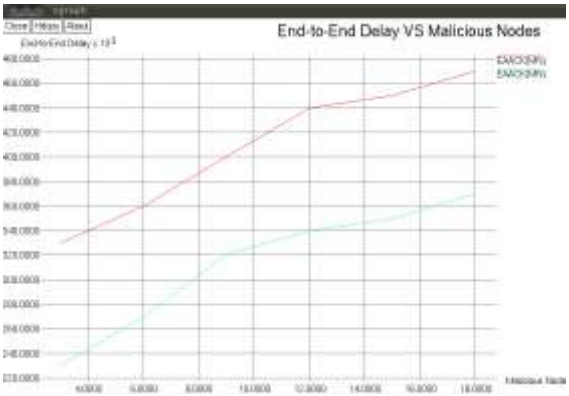

Fig.3 End-to-End Delay Vs Malicious Node

Fig.4 and Table 5compare the end-to-end delay performance of proposed SHSP-EA3ACK and existing acknowledgement based IDS scheme. SHSP-EA3ACKhas reduced end-to-end delay with the transmission range increased varied from 250 to 1000 meters when compared to the existing EAACK (DSA) protocol.Suggested new method has to reduce average delay by 41.8% than existing scheme of 600 to 1000 meters of topology area.When the transmission range increases, the connectivity among the nodes also increases, which enables the proposed method to identify more number of alternate paths which in turn reduces the delay.

Table 5 End-to-End Delay Vs. Transmission Range

Transmission Range					
Routing / Transmission Range	**250**	**400**	**600**	**800**	**1000**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.69	0.63	0.57	0.54	0.52
SHSP-EA3ACK	0.46	0.42	0.37	0.30	0.28

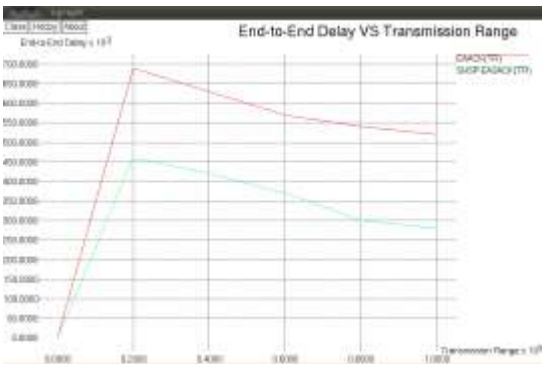

Fig.4 End-to-End Delay Vs Transmission Range

The impact of packet drop on end-to-end delay is analysed using the two algorithms proposed SHSP-EA3ACK and existing EAACK (DSA) protocols and the simulation results as shown in Fig. 5 and Table 6.Simulation results, achieve decrease in end-to-end delay obtained by 44.8% the proposed SHSP-EA3ACK when there are 5% to 30% of packet drops, proposed algorithm is capable of finding unbreakable shortest path while transmitting and receiving packets.

Table 6 End-to-End Delay Vs. Packet Drops

Packet Drop						
Routing / Packet Drop	**5%**	**10%**	**15%**	**20%**	**25%**	**30%**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.12	0.18	0.24	0.28	0.33	0.38
SHSP-EA3ACK	0.05	0.07	0.14	0.19	0.21	0.23

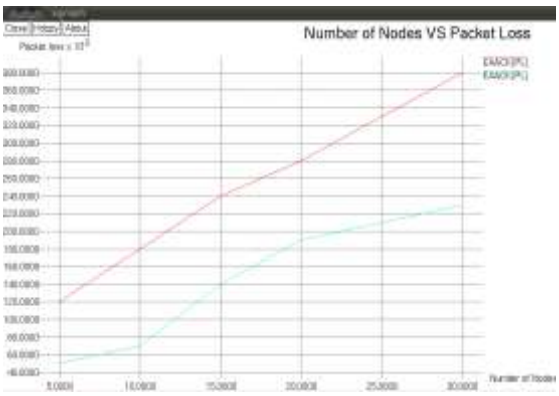

Fig. 5End-to-End Delay Vs Packet Drop

Simulation results of proposed and existing schemes compare the routing overhead performance as show in Fig. 6 and Table 7. Fig. 6 shows that SHSP-EA3ACK has reduced average routing overhead by 17.3% with the number of nodesvariedfrom 10% to 60% as compared to EAACK (DSA) scheme. If any of the intermediate nodes is found to be busy, then the proposed algorithm is able to find alternate hybrid shortest path from the previous node itself which reduces the delay.

Table 7 Routing Overhead Vs. Number of Nodes

Routing Overhead						
Routing / Number of Nodes	**10**	**20**	**30**	**40**	**50**	**60**
EAACK(DSA) (Shakshuki*et al*. 2013)	0.06	0.20	0.33	0.39	0.48	0.57
SHSP-EA3ACK	0.05	0.16	0.27	0.35	0.41	0.43

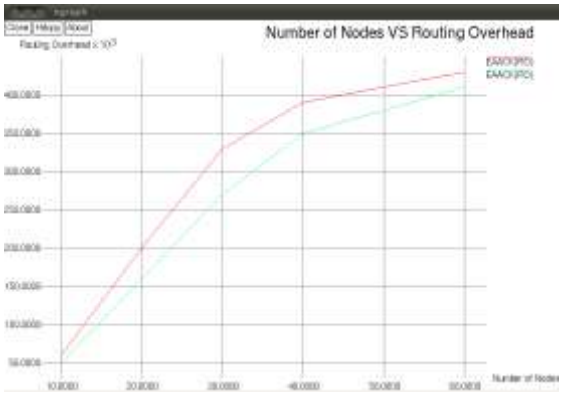

Fig.6 Routing Overhead Vs Number of Nodes

From all the above simulation results of figures and tables, it is clear that the comparison of the SHSP-EA3ACK proves that the proposed algorithm outperforms the EAACK (DSA) by providing the lowest end-to-end delay and routing overhead with the increase in the number of nodes presence of malicious nodes.

VII. SUMMARY

In the recent years of research, there has been a lot of interest in the field of acknowledgement in MANET because during the transmission, there is packet drop, link breakage,link filer (or) damage, delay in the packet if it is sent without acknowledgement. In this methodology, the new routing protocol named SHSP-EA3ACK using EAACK (DSA) is proposed to address the problem. The acknowledgement based transmission is highly secure with the lowest delay and packet dropping. This SHSP-EA3ACK provides better performance,of decreasing average end-to-end delay by 21.4% and lowering average routing overhead by 17.3% with number of nodes varied from 10 to 60 and reducing average end-to-end delay by 23.5% with varied malicious nodes from 3 to 18, minimize average end-to-end delay by 44.8% withvaried packet drop from 5% to 30% and decreasing average end-to-end delay by 38.4% with transmission range varied from 250 to 1000 meters when compared to the existing EAACK (DSA) routing protocol.Moreover, research in this chapter and the previous chapter has been dedicated to solving the delay problem during presence of malicious nodes in MANETs. Hence, the focus of the next chapter is dealing with performances comparison of various parameters with varying different topology's, number of nodes with presence of malicious nodes in MANETs.

REFERANCE

[1] AbdulsalamBasabaaa., Sheltamia, Tarek., and Shakshuki, Elhadi., (2014), Implementation of A3ACKs Intrusion Detection System Under Various Mobility Speeds, Proceedings Of 5th International Conference on Ambient System, Networking Technologies, Hasselt, Belgium, June, 571–578.

[2] Hothefa, Sh., Jassim., Salman Yussof., TiongSiehKiong., and Koh, S.P., (2009), A Routing Protocol Based on Trusted and Shortest Path Selection for Mobile Ad hoc Network, Proceedings of 9th IEEE International Conference on Communications, Malaysia, December, 547–554.

[3] Jiazi Yi., AsmaaAdnane., Sylvain David., and BenoîtParrein., (2011), Multipath optimized link state routing for mobile ad hoc networks, Ad hoc Networks, Vol. 9(1), pp. 28-47.

[4] May ZinOo, and Mazliza Othman, (2012), Analytical Studies of Interaction between Mobility Models and Single-Multi Paths Routing Protocols in Mobile Ad hoc Networks, Wireless Personal Communication, Vol. 64(2), pp. 379–402.

[5] Mohammed, Tarique., Kemal, E.T., Sasan, Adibi., and Shervin, Erfani., (2009), Survey of multipath routing protocols for mobile ad hoc networks, Journal of Network and Computer Applications, Vol. 32(6), pp. 1125-1143.

[6] Muthukumaran, N. (2017), Analyzing Throughput of MANET with Reduced Packet Loss, Wireless Personal Communications, Vol. 97(1), pp. 565-578.

[7] Nan Kang., Shakshuki, Elhadi M., and Sheltami, Tarek R., (2010), Detecting Misbehaving Nodes in MANETs, ACM Proceedings of 8th International Conference on Advances in Mobile Computing and Multimedia,Paris, France, August, 1-7.

[8] Nan Kang., Shakshuki, Elhadi M., and Sheltami, Tarek R., (2011), Detecting Forged Acknowledgements in MANETs, proceedings of 25th International Conference on Advanced Information Networking and Applications,Biopolis, Singapore, March, 488-494.

[9] Shakshuki, Elhadi M., Nan Kang., and Sheltami, Tarek R., (2013), EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, Vol. 60(3), pp. 1089-1098.

[10] Xin Ming Zhang., En Bo Wang., Jing Jing Xia., and Dan Keun Sung., (2011), An Estimated Distance-Based Routing Protocol for MANETs, IEEE Transactions on Vehicular Technology, Vol. 60(7), pp. 3473-3484.

[11] Yangcheng, H., Kannan, G., Saleem, B., Merchantand, S. N., and Desai, U. B., (2008), Route Dynamics for Shortest Path First Routing in Mobile Ad Hoc Networks, Proceedings Of 7th IEEE International Conference on Wireless Telecommunications, Pomona, CA, USA, April, 777–786.

[12] Yang, S., Cheng, H., and Wang, F., (2010), Genetic Algorithms With Immigrants and Memory Schemes for Dynamic Shortest Path Routing Problems in Mobile Ad Hoc Networks, IEEE Transactions on Systems, MAN and Cybernetics, Vol. 40(1), pp. 52-63.

[13] Yujun Zhang., Tan Yan., JieTian., QiHu., Guiling Wang., andZhongcheng Li., (2014), TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks, Ad hoc Networks, Vol. 21(2), pp. 109-122.

[14] Zafar, H., Harle, D., Andonovic, I., and Khawaja, Y., (2009), Performance Evaluation of Shortest Multipath Source Routing Scheme, IET Communications, Vol. 3(5), pp. 700 –713.