Secure Communication using Acknowledgements for MANETs

Arulkumar M

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

***Abstract*: Emerging year of one recent technology is that help and used to such as critical time successful design called Mobile Ad hoc Network (MANET) that allows to the users to access information and services anywhere regardless of their geographic location. MANET is the significant technologies used to more flowing more application conference, meeting, short time connection, natural issues like (flooding, forest fire, agriculture and military) ect., 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. But it streams including critical issue and challenges such as security, energy, delay, packet drop quality of service ect., In this research paper proposed Secure Two Acknowledgement method with MARS4 (STACK) that implement for new intrusion detection system for on-demand wireless networks. MARS4 can improve a best performance of trusted quality output to reduce transmission delay, transmission time and also increase network communication throughput help of Network Simulator-2.34 (NS2) to implement it.**

Keywords: Ad hoc, Security, Routing, STACK, MARS4.

1. Introduction

The need for wireless temporary communication facilities is rapidly increasing, because the mobile ad hoc communication service is synonymous with an ideal communication style realizing communication anytime, anywhere in the world with anyone. The accessibility of a route depends on the number of connections and the reliability of each link forming the route. Many routing metrics in terms of number of links have been proposed, such as the SPA. SPA finds a path having minimum weights to forward the packets to the destination node. SPA selection depends on direct traffic form source to destination, maximizing the network performance and minimizing the cost. Performance of the network can be enhanced through shortest path routing but it also depends upon the functionality of the routing protocol and the parameters that are selected for the shortest path routing. MANET is the one of emerging need part of natural issues in this type of network is non-fixed connect all the mobile nodes dynamically to communicate from source to destination using different types of routing protocols show in figure 1 Mobile Ad hoc Network.

Fig 1 Mobile Ad-hoc Networks

2. Routing

The routing protocols are vital role and it has to adapt quickly to the repeated changes in the ad-hoc network topology. MANET routing protocols Figure 2 are categorized into following three types. Table driven routing

protocols: these kind of routing protocols are retains the network topology information in routing tables contains a updated list of destinations and their routes by time to time swapping their routing information with nearby nodes. Routing information is usually flooded in the entire network. At any time a node wants a route to the destination it runs a suitable path finding algorithm on the topology information it retains. On-demand routing protocols: These kinds of protocols are not maintaining topology information of the network, with the help of connection establishment process nodes can obtain necessary route when it is required, and therefore this type of protocols is not exchanging the routing information time to time. Hybrid routing protocols: In this protocols both table driven, on-demand routing advantages are combined. The routing is in the beginning established with certain proactively prospected routes then it serves the demand from additionally activated nodes through reactive flooding.

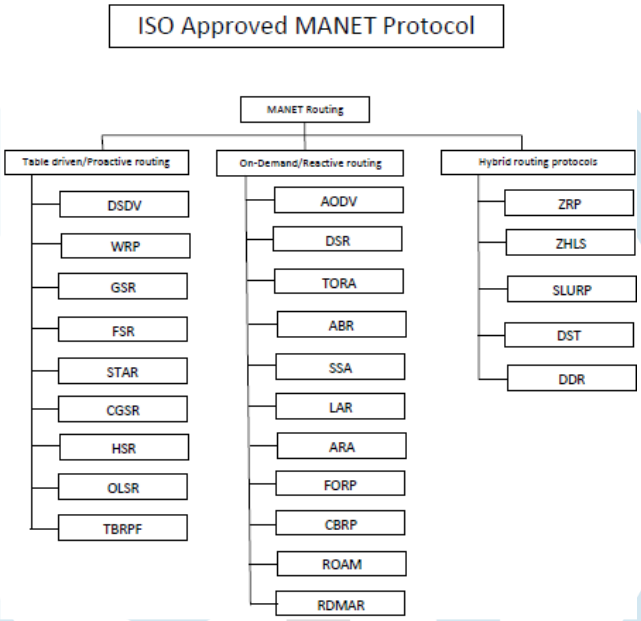

Figure 2 MANET routing protocols

3. Background

Secure routing and intrusion detection in ad-hoc networks was taken up by Anand Patwardhan et al (2005). Malicious nodes detection in AODV-based mobile ad-hoc networks was addressed by Jongoh Choi et al (2005). An acknowledgment-based approach for the detection of routing misbehaviour in MANETs was discussed by Liu et al (2007). The detection of packet dropping attack using improved acknowledgement based scheme in MANETs was done by Aishwarya Sagar et al (2010). The impact of security attacks on a new protocol for mobile adhoc networks was analysed by Sahadevaiah et al (2010). Adaptive acknowledgment intrusion detection for MANETs with node detection enhancement was analyzed by Al-Roubaiey et al (2010). Secure routing for wireless mesh network was discussed by Celia li et al (2011). Performance analysis of secure routing protocols in MANET discussed by K.Thamizhmaran et al (2012). Secure routing protocol in MANET – A survey taken by K.Thamizhmaran et al (2012). Secure intrusion detection system for MANETs was found by Shakshuki et al (2013). Implementation of A3ACK's intrusion detection system under various mobility speeds was highlighted by Abdulsalam Basabaaa et al (2014). Energy efficient routing in MANETs through edge node selection using ESPR algorithm was discussed by Prabu and subramani (2014). Performance evaluation of EA3ACK in different topology's using EAACK for MANET highlighted by K.Thamizhmaran (2016). Performance analysis of energy efficient enhanced adaptive 3-acknowledgement (EE-EA3ACK) using ECC in MANET analyzed by K.Thamizhmaran et al (2017). Comparison and parameter adjustment of topology based (S-EA3ACK) for MANETs done by K.Thamizhmaran et al (2017). Performance analysis of on-demand routing protocol for MANET using EA3ACK algorithm addressed by K.Thamizhmaran et al (2017). Reduced end-to-end delay for MANETs using SHSP-EA3ACK algorithm proposed by K.Thamizhmaran et al (2017). However, all these algorithms address only the security problem because misbehavior attacks due to topology changes rapidly in MANETs

due to the characteristics of wireless networks. The proposed approach scheme STACK with help of MARS4 hybrid cryptography is also based on this assumption to provide secure transmission with minimum delay.

4. Problem Identification

The dynamic nature of MANETs requires the routing protocols to refresh the routing tables frequently and suffer from transmission contention time delay and congestion with packet dropping that are the results of the broadcasting nature of radio transmission since a node in MANETs 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 MANETs is the one in finding a route without malicious nodes in the shortest path. This paper aims to provide unbreakable route for secure transmission with the shortest path. So a new routing algorithm named STACK using ACK with hybrid cryptography is proposed. This STACK provides better performance compared to the existing ACK and also reduces routing delay and packet dropping without any misbehavior at intermediate nodes.

5. Proposed work

In STACK mode, the three consecutive nodes (i.e., A, B, C) work in a group to overcome the drawbacks of watchdog scheme in the network. Node A first sends out STACK data packet P1(S) to node B. Then, node B forwards this packet to node C. When node C receives P1(S), as it is the third node in this three-node group, node C is required to send back a STACK acknowledgement packet P1 (A) to node B. Node B forwards this P1 (A) back to node A. If node A does not receive this acknowledgement packet within a predefined time period, both nodes B and C are reported as malicious. This process is shown in Figure 3.

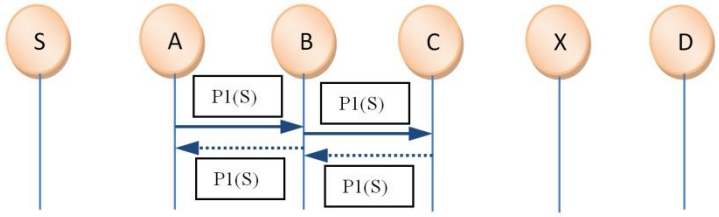

Fig. 3 STACK

Procedural Steps of STACK Algorithm

- STACK processing starts with hybrid cryptography.
- Hello packet transmission from source to destination through intermediate nodes.
- Destination node sends ACK message to source node in same route through intermediate nodes.
- If source node receives this acknowledgement packet within a predefined time period, then data transmission will be start.
- If node A does not receive this acknowledgement packet within a predefined time period, then the intermediate nodes are marked as malicious nodes.
- Switch to TACK. Send acknowledgement packet through intermediate node, this model to detect if there are any receiver collision, false misbehaviour nodes and limited transmission power in the route.
- Out of the three consecutive nodes in the TACK, the third node is required to send an ACK packet to the temporary source node same rout with opposite direction.
- If node A receives this acknowledgement packet within a predefined time period, then data transmission will be start, otherwise both nodes B and C are reported as malicious. when malicious report is received to the source node than, source node switch to MRA.
- MRA checks authentication (secure value) to all nodes and if MAR receives this acknowledgement packet within a predefined time period, then the data transmission will be start, otherwise marked as misbehaviour node.
- Transmit the data in the alternate path to the destination, and go to step1.

Procedural Steps of Hybrid Cryptography (MARS4 Algorithm)

- Now MAJE4 and RSA can be combined to have MARS4 as a very efficient security solution. It is assu
- med that A is the sender of a message and B is the receiver. MARS4 is designed to work as follows.
- A encrypts the original message (PT) with the help of MAJE4 and the symmetric key (K1) and forms the cipher text (CT).
- Again encrypt symmetric key K1 to (K2) of B using RSA.
- B now uses the RSA algorithm and its private key (K3) to decrypt symmetric key K1.
  Then B uses K1 and the MAJE4 algorithm to decrypt the CT for the original plain text (PT).

STACK consists of three major parts, namely, ACK, 2-ACK, Misbehaviour Report Authentication (MRA). With the introduction of hybrid cryptography algorithm MARS4 prevents the attacker from forging acknowledgement packets and also simulate help of following simulator called NS 2.34 is used to test the Intrusion Detection System's (IDSs) 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 1, the following are the simulation parameters used for the analysis of routing protocol with hybrid shortest path algorithm.

Table 1 Simulation parameters

Parameter	Values
Examined protocol	STACK-MARS4
Application traffic	CBR
Transmission range	1000m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	900s
Number of nodes	60
Area	1000x1000m
Maxi. number of malicious nodes	18

6. Result and Discussion

In this work, the malicious nodes are provided the ability to forge acknowledgment packets. This way, 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 STACK is designed to tackle four of the six weaknesses of watchdog scheme, namely, receiver collision, limited transmission power, false misbehaviour, and partial dropping.

Table 2 Results of Parameter Values

End–to–End Delay						
Delay / NN	10	20	30	40	50	60
TACK	0.57	0.52	0.47	0.41	0.33	0.24
STACK-MARS4	0.48	0.44	0.39	0.31	0.24	0.17
Malicious Node						
Delay / MN	3	6	9	12	15	18
TACK	0.33	0.36	0.40	0.44	0.45	0.47
STACK-MARS4	0.23	0.27	0.32	0.34	0.35	0.37
Transmission Range						
Delay / TR	0	250	400	600	800	1000
TACK	0	0.69	0.63	0.57	0.54	0.52

STACK-MARS4	0	0.46	0.42	0.37	0.30	0.28
Packet Drop						
Delay \ PD	5%	10%	15%	20%	25%	30%
TACK	0.12	0.18	0.24	0.28	0.33	0.38
STACK-MARS4	0.05	0.07	0.14	0.19	0.21	0.23
Routing Overhead						
RO \ NN	10	20	30	40	50	60
TACK	0.06	0.20	0.33	0.39	0.48	0.57
STACK-MARS4	0.05	0.16	0.27	0.35	0.41	0.43

MN=Malicious Node, TR=Transmission Range, PD=Packet Drop, RO= Routing Overhead, NN=Number of Nodes

End–to–end delay when the number of nodes is increased from 10 to 60. According to table 2, it is clear that in all acknowledgement-based IDSs, the proposed scheme STACK-MARS4 surpassed the performance of TACK in minimizing end-to-end delay by 8.5% 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. It is observed from Table 2 that when compared with TACK algorithm, STACK-MARS4 decreases the delay by 9.5% with increase in the number of malicious nodes from 3 to 18 out of 60 nodes. If malicious node is detected, immediately the STACK-MARS4 algorithm finds alternate shortest route in between the sender and receiver.

Transmission range is varied from 250 to 1000 meters and simulation is carried out to calculate the end–to-end delay using TACK & STACK-MARS4 methods. The obtained results are given in table 2. It is clear from the simulation results that the DSR scheme achieves the best performance, as it does not require acknowledgment scheme to detect misbehaviours. In case of the IDSs, STACK-MARS4 has the lowest delay in comparison with TACK, when there are 250 to 1000 meters of transmission ranges. When transmission range increases, connectivity among the nodes also increases, which enables the proposed method to identify more number of alternate paths which in turn reduces the delay.

Finally routing overhead is analyzed using the two algorithms when the total number of nodes is varied from 10 to 60 and the simulation results are shown in table 3. Simulation results reveal that the proposed algorithm reduces the routing overhead by 6% than TACK algorithm. 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.

From the entire above table 2, it is clear that the comparison of the STACK-MARS4 illustrate that the proposed algorithm outperforms the TACK by providing lowest end-to-end delay, packet drop and routing overhead with increase in the number of nodes.

7. Conclusion & Future Work

In the recent research years, there has been a lot of interest in the field of acknowledgement in MANETs, because during the transmission, there is drop (or) delay in the packet if it is sent without acknowledgement. In this paper, the new routing protocol named STACK-MARS4 using TACK is proposed to address the problem. Acknowledgement based transmission is highly secure with the lowest delay and packet dropping. This STACK-MARS4 provides better performance compared to the existing TACK routing protocol by decreasing end-to-end delay by 8.5% lowering routing overhead by 6% and reducing packet drop by 10.7% compared to the existing TACK routing protocol. To enhance the merits of this research work, there is a plan to investigate the following issues in the future. However, the same concept can be applied in satellite to reduce end-to-end delay in the route and reduce packet loss, Possibilities of adopting secure quality oriented techniques to further improve the network performance of quality.

Reference

1. Anand Patwardhan and Iorga, "Secure routing and Intrusion Detection in Ad hoc networks", in Proc. 3rd Int. Conf. Pervasive Computer Communication, pp.191–199 (2005).
2. Balakrishnan, et al, "TWOACK: preventing selfishness in mobile ad hoc networks", Proc. Int. Conf. on Wireless Communications and Networking, vol.4, no.10, pp. 2137-2142 (2005).
3. Jongoh Choi, et al, "Malicious Nodes Detection in AODV- Based Mobile Ad Hoc Networks", GESTS Trans. Comp. Science and Engg, vol.18, no.1, pp.49-55 (2005).
4. Prabu, K. and Subramani, A. "Performance comparison of routing protocol in MANET", Int. J. of Adv. Research in Com. Sci. and Soft Engg., Vol. 2, No. 9, pp.388–392 (2012).
5. K. 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 (2012).
6. D. Raj Vikram Singh1, S. Subhash Kumar Kesarwani and K.Thamizhmaran "Secure Routing Protocol in MANET – A Survey", International Journal of Engineering Journals and Tech, Vol. 3, No. 3, pp. 22-29, (2012).
7. Shakshuki, et al, "EAACK-A Secure Intrusion: Detection System for MANETs", IEEE Trans on industrial electronics, vol. 60, no. 3, pp. 1089-109 (2013).
8. Prabu, K. and Subramani, A. "Energy efficient routing in MANET through edge node selection using ESPR algorithm", Int. J. Mobile Network Design and Innovation, vol. 5, no. 3, pp.166–175 (2014).
9. Abdulsalam Basabaaa, et al, "Implementation of A3ACKs intrusion detection system under various mobility speeds", in Proc. 5th Int. Conf. on Ambient Systems, Networks and Technologies, pp.571-578 (2014).
10. K. Thamizhmaran "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 (2016).
11. K.Thamizhmaran, M.Anitha and Alamelunachippan "Performance Analysis of energy-Efficient Enhanced Adaptive 3- Acknowledgement (EE-EA3ACK) Using ECC in MANET", ARPN, Vol. 12, No. 9, pp. 2901-2912 (2017).
12. K.Thamizhmaran, M.Anitha and Alamelunachippan "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 (2017).
13. 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 (Inderscience), Vol. 7, No. 2, pp. 88-100 (2017).
14. K.Thamizhmaran, M.Anitha and Alamelunachippan "Reduced End-to-End Delay for MANETs using SHSP-EA3ACK algorithm", Journal on Communication Engineering and System, Vol. 7, No. 3, pp. 8-15 (2018).