Global Journal of Pure and Applied Mathematics (GJPAM) ISSN 0973-1768 Volume 12,Number 4 (2016)

Detecting misbehaving nodes in MANET using EA3ACK algorithm

K. Prabu
Department of Computer Science,
Thiruvalluvar University Constituent College,
Tittagudi, Tamilnadu, India – 606 106,
E-mail: kprabu.phd@gmail.com

*K. Thamizhmaran**
Department of Electrical Engineering,
Annamalai University,
Chidambaram, Tamilnadu, India - 608 002,
E-mail: tamil10_happy@rediff.com

Abstract **– Wireless networking is an emerging technology that allows users to access information and services anywhere regardless of their geographic areas over the past few years, with the trend of mobile computing. Mobile Adhoc Network (MANET) has become one of the most important wireless communication mechanisms among all, unlike traditional network. MANET does not have a fixed infrastructure. Every single node in the MANET works as both receiver and transmitter. Each node directly communicates with others when they are both within their communication ranges. All nodes work as routers and take path in discovery and maintenance of routes to other nodes in the network. In this paper proposed a new routing algorithm named Enhanced Adaptive 3 Acknowledgement (EA3ACK) using EAACK with hybrid cryptography is (MARS4) specially designed for MANET. This hybrid cryptography a two key method namely MARS4 which is a combination of RSA and MAJE4 employed to reduce the routing overhead. The proposed EA3ACK algorithm provides efficient secured transmission compare to existing EAACK algorithm.**

Keywords: EA3ACK, IDS, MARS4, Cryptography, Security, MANET, Throughput.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANET) represent a new form of communication consisting of mobile wireless terminals where it is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. As shown in the fig.1.1 nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified node in the network. MANET were wireless multi-hop networks without any fixed infrastructure and centralized administration, in contrast to today's wireless communications, which is based on fixed, pre-established infrastructure.

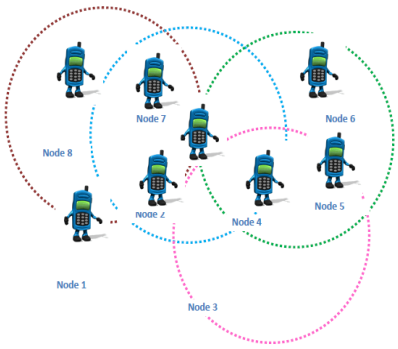

Figure 1.1 Mobile Adhoc Networks

All networking functions, such as determining the network topology, multiple accesses, and routing of data over the most appropriate paths, must be performed in a distributed way. These tasks are particularly challenging due to the limited communication bandwidth available in the wireless channel.

II. BACKGROUND

2.1 Routing Protocol

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. The two main types of routing: Static routing and dynamic routing.

Generally, there are two different stages in routing; they are route discovery and data forwarding. In route discovery, route to a destination will be discovered by broadcasting the query. Then, once the route has been established, data forwarding will be initiated and sent via the routes that have been determined. The power consumption, route relaying load, battery life, and

*Corresponding author.

This paper was presented by the second author in the National Conference on AMASE-2016 conducted in Department of Mathematics, University College of Engineering Pattukkottai, Thanjavur, Tamil Nadu, India, on 22nd January 2016.

reduction in the frequency of sending control messages, optimization of size of control headers and efficient route reconfiguration should be considered when developing a routing protocol.

Proactive approach every node generates routing information periodically to maintain and construct routing tables even if there is no data traffic to deliver. Information contained in routing tables, is updated when the topology changes. Thus, every node maintains routing information to every other node in the network. Proactive routing protocols may use either hop-by-hop or source routing strategies to forward data traffic. The performance of the network degrades due to the exchange of control traffic messages, but the packets experience less latency because the routes are always constructed and maintained for eventual data traffic. Proactive protocols work better in networks with low mobility.

Reactive routing protocols discovery and maintenance of routes are delayed until necessary. When a given node needs to send a packet to any other node in the network, the sender node initiates the process to construct a path to reach the destination. To discover a route, a node floods the route request messages through the network. When a node with a route to the destination (or the destination itself) is reached, a route replay message is sent back to the source node. Reactive protocols can be classified into two categories: source routing and hop-by-hop routing.

Hybrid routing protocol is a combination of proactive and reactive routing protocol. Zone-based Hierarchical Link State (ZHLS) is a typical example. According to ZHLS routing protocol, the entire network is divided into several non-overlapping zones. If the source and destination nodes are within the same zone, ZHLS works as a passive routing protocol.

2.2 Cryptography

Cryptography technique has a long and fascinating history. Completed in 1963, the Kahn's book covers the most important history of cryptography technique. From 4,000 years ago by the Egyptians, to the two world wars in the twentieth century, the cryptography technique has been widely served as a tool to protect secrets. With the development of Internet, the security of communication has become more important than ever. Many researchers and scientists have contributed their countless time and efforts in this area since then. Among all of them, it is believed the most significant development was in 1976 when Diffie and Hellman published the paper "New Directions in Cryptography", in which they first introduced the concept of public-key cryptography. Although no practical implementation was provided along with the paper, the idea had since then attracted various attentions and interests. Two years later, in 1978, Rivest, Shamir and Adleman proposed the first practical public-key encryption and signature scheme, which we now referred to as RSA. Later after that, the 1980s has witnessed much more advancement in this area but none of them rendered RSA as insecure. EIGamal in 1985, found another class of powerful and practical public-key schemes. These are also based on the discrete logarithm problem. The Digital Signature Standard (DSA) scheme announced in 1994 was developed based on the EIGamal public key scheme. Cryptographic techniques are typically divided into two generic types: symmetric-key and public-key.

III. PROPOSED SYSTEM

A) RSA

RSA is computationally easy for a party B to generate the key pair (Public key KSb, Private key KRb). It is computationally easy for a sender A, knowing the public key KSb and the message to be encrypted M, to generate the cipher text C=EKSb (M). It is computationally easy for the receiver B, to decrypt the resulting cipher text using the private key to recover the original message *M=DKRb(C) =DKRb [EKSb (M)]*. It is also computationally infeasible for an opponent, knowing the public key KSb, and a cipher text C, to recover the original message M. The encryption and decryption functions can be applied in either order. M=DKRb [EKSb(M)]= DKSb[EKRb(M)]

- Choose two higher prime numbers P and Q, and find N=P*Q.
- Select the encryption (public key) E & Select the decryption (private key) D. the following equation is true: (D*E) mod (P-1) * (Q-1) = 1
- Encrypt the PT to CT = PTE mod N
- Send CT to the receiver.

B) MAJE4

The same as that for a One-time-Pad cipher, which encrypts by XOR' of the plain text with a random key. But for a One-Time-Pad Cipher it is required to have a key of the same size as the plain text, which makes it impractical for most applications. While the stream ciphers require only a short random key.

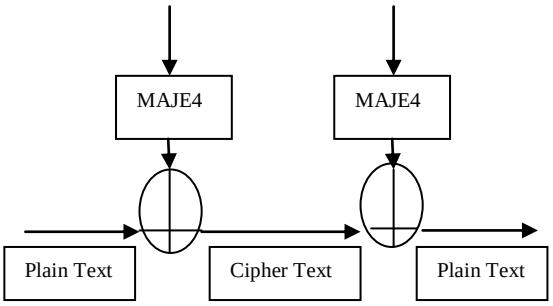

Figure 3.1 MAJE4

C) MARS4

Now MAJE4 and RSA can be combined to have MARS4 as a very efficient security solution. Assume that A is the sender of a message and B is the receiver. MARS4 is designed to work as follows.

1) A encrypts the original message (PT) with the help of MAJE4 and the symmetric key (K1) and forms the cipher text (CT).
2) Encrypt K1 (CT) to (K2) of B using RSA.
3) B now uses the RSA algorithm and its private key (K3) to decrypt K1.
4) Then B uses K1 and the MAJE4 algorithm to decrypt the CT for the original plain text (PT).

IV. METHODOLOGY

FLOW DIAGRAM

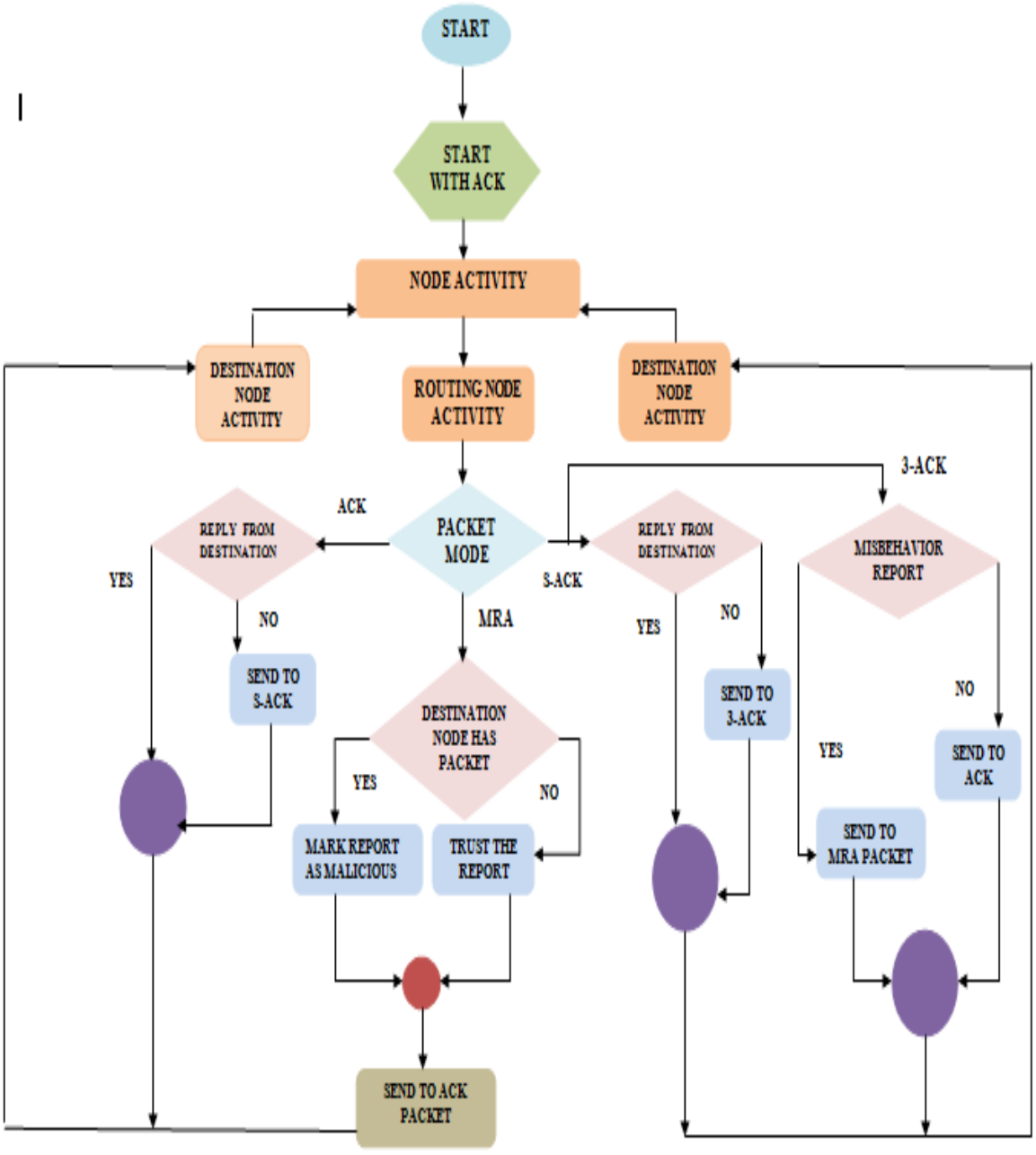

Figure 4.1 Flow diagrams for EA3ACK

In this section, we describe our proposed EA3ACK scheme in detail. The approach described in this research paper is based on previous work (2), where the backbone of EA3ACK was proposed and evaluated through implementation. We extend it with the introduction of MARS4 Hybrid cryptography to prevent the attacker from forging acknowledgment packets. EA3ACK is consisted of four major parts, namely, ACK, secure ACK (S-ACK), 3-ACK and misbehaviour report authentication (MRA). In order to distinguish different packet types in different schemes In EA3ACK, we use 3 b of the different types of packets. Details are listed in Table 5.1 Fig. 5.1presents a flowchart describing the EA3ACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to two different keys (public and private) by its one key for sender and verified another key by its receiver.

V. RESULT AND DISSCUSSION

Simulation Configurations

In this section, we evaluate the performance of routing protocol of MANETs in an open environment. The simulations were carried out using network simulator (NS 2.34). We are simulating the mobile ad hoc routing protocols using this simulator by varying the number of nodes. The IEEE 802.11 distributed coordination function (DCF) is used as the medium access control protocol. The traffic sources are UDP. Initially nodes were placed at certain specific locations. The simulation parameters are specified in Table 5.1.

Parameters	Values
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
Node beacon interval	0.5 (seconds)
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	500 sec

Table 5.1 Simulation parameters

In this section, malicious nodes drop all the packets that pass through it. Fig 5.1 and Table 5.1 shows the simulation results that are based on PDR.

Packet Delivery Ratio					
Routing / Malicious Node	**0%**	**10%**	**20%**	**30%**	**40%**
DSR	1	0.82	0.73	0.68	0.66
WATCHDOG	1	0.83	0.77	0.70	0.67
AACK	1	0.96	0.96	0.93	0.92
TWOACK	1	0.97	0.96	0.92	0.92
THREEACK	1	0.96.5	0.96	0.91	0.92
EAACK(RSA)	1	0.96	0.97	0.92	0.92
EEACK(DSA)	1	0.96	0.97	0.93	0.91
EA3ACK	1	0.97	0.97	0.96	0.95
Routing Overhead					
Routing / Malicious Node	**0%**	**10%**	**20%**	**30%**	**40%**
DSR	0.02	0.023	0.023	0.022	0.02
WATCHDOG	0.02	0.025	0.025	0.023	0.023
AACK	0.03	0.23	0.32	0.33	0.39
TWOACK	0.18	0.4	0.43	0.42	0.51
THREEACK	0.19	0.43	0.45	0.42	0.50
EAACK(RSA)	0.16	0.3	0.37	0.47	0.61
EEACK(DSA)	0.15	0.28	0.35	0.44	0.58
EA3ACK	0.14	0.26.5	0.32	0.40	0.55
Throughput					
Routing / Malicious Node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK(RSA)	0	0.25	0.38	0.50	0.54
EEACK(DSA)	0	0.27	0.40	0.53	0.57
EA3ACK	0	0.37	0.50	0.63	0.58
Energy					
Routing / Malicious Node	**0%**	**10%**	**20%**	**30%**	**40%**
EEACK	1	0.95	0.89	0.80	0.76
EA3ACK	1	0.92	0.84	0.76	0.72

Table 5.2 Performance Comparison.

In Fig. 5.1 and Table 5.2 we observe that all acknowledgment-based IDSs our proposed scheme EA3ACK surpassed EAACK performance by above 95% when there are 30% and 40% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes, EA3ACK, are able to detect misbehaviors with the presence of receiver collision, limited transmission power and partial dropping.

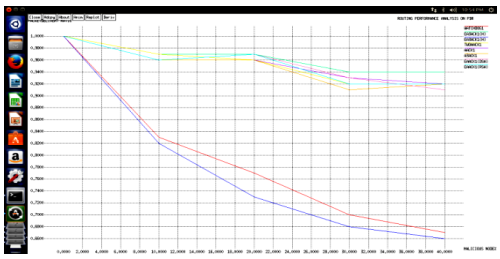

Figure 5.1 PDR vs. Malicious Nodes

Simulation results are shows that fig.5.2 and table 5.2. We observe that DSR scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors. For the rest of the IDSs, EA3ACK

has the lowest overhead when there are 10% to 30%. Although EA3ACK requires public and private key at all acknowledgment process.

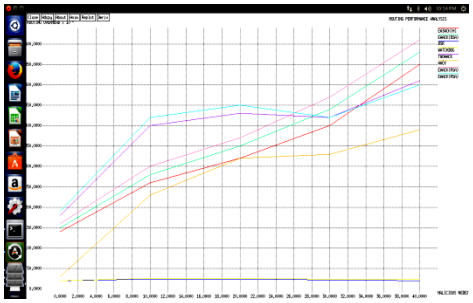

Figure 5.2 Routing Performance vs. Malicious Nodes

Simulation results are shows that fig 5.3 and table 5.2 shows that comparison of the EAACK with corresponding RSA and DSA algorithm since on along with EA3ACK where it shows the throughput is increase with increase in the number of malicious nodes on while 30% and 40%.

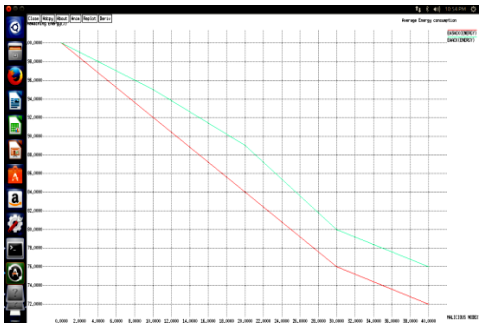

Figure 5.3 Average Energy Consumption vs. Malicious Nodes

Simulation results are shows that fig 5.4 and table 5.2 shows that our proposed EA3ACK deceasing the remaining energy with increasing malicious nodes compare to the existing algorithm.

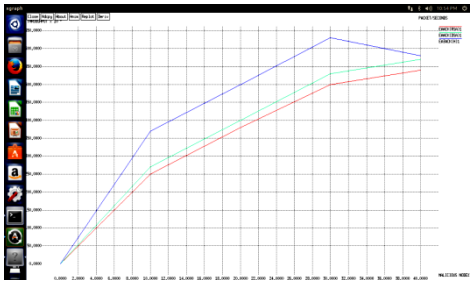

Figure 5.4 Packer per/sec vs. Malicious Nodes

Simulation results are shows that the all above figure and Table shows that the comparison of the EAACK with corresponding RSA and DSA algorithm since on along with EA3ACK with hybrid cryptography where it shows the throughput is increase with increase in the number of malicious nodes on while.

VI. CONCLUSION

In the recent research year there has been a lot of interest within the field of cryptography in MANET. Because during the transmission drop (or) attack the packet without the acknowledgement. So acknowledge based transmission is very safe and high security. The motivation for our work is to develop an Intrusion Detection System (IDS) scheme able to detect misbehaving node in case of collision, limited transmission power and false misbehavior report. We demonstrated the performance of our proposed scheme named EA3ACK with hybrid cryptography using EAACK through an evaluation in the network simulator environment. This EA3ACK provide better performance compare to existing EAACK routing protocol and also improved packet delivery ration, improved throughput, and reduced routing overhead compare to existing EAACK routing protocol. Finally EA3ACK shows that the result of proposed scheme is effective in detecting misbehaving nodes in MANET.

REFERENCES

[1] Nan Kang, Elhadi et.al “Detecting Misbehaving Nodes in MANETs”, International conference on Advanced Information Networking and Applications, pp.488-494, 2010.

[2] Prabu, K. and Subramani, A. (2012) ‘Performance comparison of routing protocol in MANET’, Int. J. of Adv. Research in Com. Sci. and Soft Engg. (IJARCSSE), Vol. 2, No. 9, pp.388–392, 2012.

[3] Elhadi, M. Shakshuki, Nan Kang and Tarek R. Sheltami “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Trans on industrial electronics, vol. 60, no. 3, pp.1089-1098, 2013.

[4] Abdulsalam Basabaaa, et al, “Implementation of A3ACKs intrusion detection system under various mobility speeds”, 5th International Conf. on Ambient Systems, Networks and Technologies, pp.571-578, 2014.

[5] Sheena Mathew and K.Paulose Jacob “A Novel Fast Hybrid Cryptographic System: MARS4”, IEEE, vol.2, no.4, 2006.

[6] S. Subasree and N. K. Sakthivel “Design Of a New Security Protocol Using Hybrid Cryptography Algorithms”, IJRRAS vol.2 no.2, pp., 2010.

[7] Nidal Nasser and Yunfeng Chen “Enhanced Intrusion Detection System for Discovering Malicious Nodes n in Mobile Ad hoc Networks”, IEEE Comm Society, 2007.

[8] K. Liu, J. Deng, P. K. Varshney et al, “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,” IEEE Trans. Mobile Comput., vol.6, no.5, pp.536–550, 2007.

[9] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, vol.4, no.10, pp. 2137-2142, 2005.

[10] Al-Roubaiey, A.; Sheltami, T.; et al “AACK: Adaptive Acknowledgment Intrusion Detection for MANET with

Node Detection Enhancement," 24th IEEE Conf. on AINA, pp.634-640, 2010.

[11] D. Johnson, D.A. Maltz and J. Broch, "The dynamic source routing protocol for mobile ad hoc networks", Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, 1998.

[12] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in Mobile Ad hoc Networks: Challenges and Solutions", UCLA Computer Science Department, 2010.

[13] Jongoh Choi, Si-Ho Cha, GunWoo Park, and JooSeok Song. "Malicious Nodes Detection in AODV-Based Mobile Ad Hoc Networks", GESTS Trans. Comp. Science and Engr., Vol.18, No.1 pp.49-55, 2005.

[14] A Rajaram, and S. Palaniswami, "Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol" (IJCSIT) Int. Journal of Com Sci and Information Technologies, Vol.1, no.2, pp., 2010.

[15] Aishwarya Sagar Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI, Vol.7, No.4 (1), 2010.