Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ECC BASED MALICIOUS NODE DETECTION SYSTEM FOR MOBILE ADHOC NETWORK

[1]V. ANJANA DEVI, [2]R.S. BHUVANESWARAN
[1]Associate Professor, St.Joseph's College of Engineering, Chennai, India
[1]Research Student, Anna University, Chennai , India
[2]Associate Professor, Anna University, India
E-mail: [1]anjanadevi_anne@yahoo.com

ABSTRACT

An ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Due to MANET characteristics, nodes in MANET are easily compromised by the adversaries. In this paper an innovative scheme is proposed to monitor and detect the malicious nodes without compromising the network performances. The major contribution is to alleviate the Watchdog (IDS for MANET) issues such as limited transmission power, packet dropping, receiver collision and false misbehavior reports generation. The proposed approach is an acknowledgement based, in which each acknowledgement packet is digitally signed with an Elliptic Curve Cryptography (ECC) algorithm for authenticating the acknowledgement packets. Simulation results demonstrate that the proposed scheme offer more security and improve the network performances than earlier IDS approaches. The proposed system improves the packet delivery ratio and also minimizes the routing overhead even in the presence of 40% malicious nodes in the network.

Keywords: *Intrusion detection System, Mobile adhoc Network, Elliptic Curve Cryptography, Attacks, Acknowledgement.*

1. INTRODUCTION

MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure less network. An ad-hoc network[6] is self-organizing and adaptive in nature. Due to minimal configuration and quick deployment, MANET can be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. In MANET each node will act as the node and also as a router. Hence message routing is a problem in a decentralized environment where the topology fluctuates. MANET suffered with several weaknesses such as limited bandwidth, battery power, computational power, and security. MANET is more vulnerable than wired network due to mobility of nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks[12][15]. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks.

Due to MANET distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANET. In such case, it is crucial to develop an intrusion-detection system (IDS)[13] for MANET. An intrusion detection system (IDS)[2] can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Depending on the detection techniques used, IDS can be classified into Signature or misuse based IDS, Anomaly based IDS and Specification based IDS. The signature based IDS uses pre-known attack scenarios and compare them with incoming packets traffic. The anomaly based IDS attempts to detect activities that differ from the normal expected system behavior. The specification based IDS are hybrid of both the signature and the anomaly based IDS.

The rest of the paper is organized as follows. In section 2 various intrusion detection system along with MANET behaviors are briefly discussed and compared with the previous works. In section 3,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

problem definition is explained and in section 4, the proposed work with the system model is illustrated. In section 5 the performance evaluation of the proposed work is discussed with results. Conclusions and References are illustrated in the following sections 6 and 7 respectively.

2. RELATED WORKS

Mobile ad hoc networks (MANET) are the combination of wireless communication by a high level of node mobility[6]. Due to the advantages such as flexibility and mobility, MANET is applied in many areas such as Military communication, Emergency services need for Disaster recovery, Education and Entertainment, etc. The specific characteristics of MANET impose many challenges for security and Intrusion-Detection Systems (IDS). Intrusion Detection is the process of identifying interruption or abusing activities in the system. An **Intrusion-Detection System** (**IDS**) is a device or software function that monitors network or system behaviors for malevolent activities that abuse the security policy within the system. It is complex to detect routing attacks due to MANET characteristics [3][4][13]. So, the IDS require a scalable design to accumulate reasonable facts to discover those attacks effectively.

Intrusion detection has been efficiently used to discriminate attacks in wired networks that can afford a second line of protection. IDS is very important, because ad-hoc networks will be deployed in hostile environments in which valid nodes can be captured and used by the adversaries [11]. Types of intrusion-detection systems are stated by the source of the audit information. Based on that, IDS may be classified into Host-based IDS, Network-based IDS and Distributed IDS. IDS can be classified according to the detection techniques as Signature based detection system, Anomaly based detection system and specification based detection system. In[18], the author discussed about specification based IDS using Genetic Algorithm which analyses the behavior of every node and provides details about the attack. Use of Fuzzy Inference System (FIS) in the design of IDS is proven to be efficient in detecting routing attacks in MANET[1][2]. In this section, the following schemes Watchdog [6], TWOACK [7], AACK [8] and EAACK [9] are discussed.

One of the existing IDS approaches, Watchdog's [5][6] was not succeeded to discover mischievous nodes in the presence of receiver collision, limited transmission power, false misbehavior, and partial dropping. A malicious node might divide the network and succeeded with the path including misbehaving nodes. The false misbehavior report can be caused by malevolent attackers who incorrectly report innocent nodes as malicious. This attack can be dangerous to the entire network when the attackers halt down adequate nodes and thus source a network division.

In order to solve the issues presented in the watchdog's scheme the other IDS approach TWOACK has proposed to mitigate the unpleasant role of misbehaving nodes [7]. It was implemented on top of source routing protocol such as DSR and the packet derives its route from the source route established for the corresponding data packet. The fundamental responsibility of TWOACK scheme is that, the sender node will get a two-hop acknowledgement TWOACK for every packet transmission over the next hop to designate that the data packet has been received successfully [9]. This scheme has answered the issues of receiver collision and limited transmission power problems and it sufficiently increased the network overhead and degraded the network performance.

A network layer acknowledgment-based Adaptive ACKnowledgment (AACK) [8] scheme was projected to overcome watchdog weaknesses such as collisions and limited transmission power and also to improve the problems presented with TWOACK scheme. The main purpose of this scheme is to identify the exact misbehaving node on the misbehaving links. But in this scheme of IDS the sources took longer paths for transmission and which led to higher end-to-end delay and also it increased more the detection rate that sufficiently increase the routing overhead due to more route discovery phases.

Enhanced Adaptive ACKnowledgment (EAACK) [9] is specially designed for MANETs. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). ACK is basically an end-to-end acknowledgment scheme. Within a predefined time period, if node S receives Ack packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives S-ACK data packet, as it is the

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet to node F2. Node F2 forwards it back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious and misbehavior report will be generated by node F1 and sent to the source node S. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes to detect misbehaviors in the network. In order to make sure the integrity, EAACK requires all acknowledgment packets to be digitally signed before they are sent out. The Digital Signature algorithm is adopted for authentication process. But if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

The main contribution of this work is to conquer the frequent problems presented with MANET such as network overhead, packet dropping, receiver collision and false misbehavior report. Network Overhead due to the acknowledgment process is prevented in the proposed system by considering three consecutive nodes for transmission and receiving acknowledgments. The packet dropping attack [9] is dealt with by buffering the recently forwarded packets to the next hop that is when the malicious node identified which is blocked [10], and then forwards the temporarily stored packets in buffer through an alternative path to the consequent node. By using this technique the system can resolve the packet dropping attack in an efficient manner. The receiver collision and false misbehavior report generation attacks can also be resolved by the proposed system.

3. PROBLEM DEFINITION

The proposed scheme is designed to address the Watchdog issues such as receiver collision, limited transmission power, false misbehavior reports and packet dropping. In this section, a detailed description about these issues were discussed.

An example of receiver collisions is shown in Fig.3.1. Node A forwards packet1 to node B and it overhears whether node B forwards the packet to node C . Node B forwards packet1 to node C. At the same time node X forwards packet2 to node C. Hence packet1 and packet2 will collide at node C.

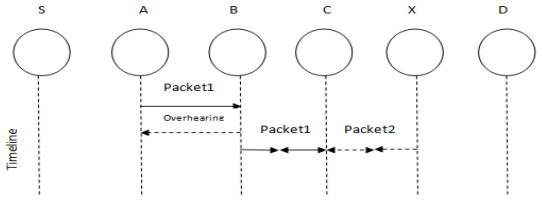

Fig. 3.1. Receiver Collision: Both nodes B and X are trying to send the Packet1 and Packet2 respectively to the node C at the same time

In the case of limited transmission power, in order to preserve its own battery resources , A node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by the true recipient.

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving, as shown in Fig. 3.2. Due to the open medium and remote distribution of typical MANET, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

The malicious nodes in the network will not forward the entire packets to its neighbor. It will drop all packet since the malicious nodes are selfish nodes. The proposed scheme is designed to evade all these above mentioned weaknesses in MANET. The scheme is integrated with digital signature in order to ensure the integrity and authenticity of the acknowledgement packets.

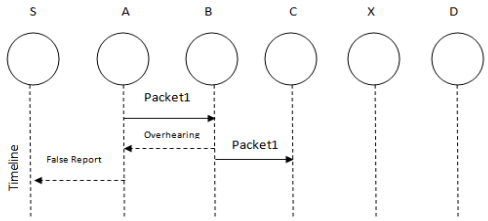

Fig. 3.2. False Misbehavior Report: Node A sends back a misbehavior report even though B forwards the packets to node C.

4. ECC BASED MALICIOUS NODE DETECTION SYSTEM

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The proposed system mainly designed to evade the issues such as limited transmission power, packet dropping, receiver collision and false misbehavior reports. The system model is shown in Fig.4.1.

4.1 System Model

The first step in this scheme is to select the energy efficient path which is taken by the following mechanism; when the source and destination are selected, the system will choose energy efficient nodes in order to make the energy efficient path between them for transmitting packets [11]. If the node within the source node's transmission range with highest energy containing for transmission and if it is nearer (having lesser distance) from the destination node then that node will be elected as an energy efficient node which is the first intermediate node N1 from the source node. The next intermediate node also selected based on same scenario. This process is repeated until the destination is reached and the path through these energy efficient nodes is called as the energy efficient path. The distance is calculated by the Euclidean distance formula. According to the distance and energy of the nodes, energy efficient transmission takes place between the selected nodes for packet transmission. The flowchart describing the proposed scheme is shown in Fig.4.1.

System assumes that N number of nodes is randomly arranged in a wireless ad hoc network. In this scheme, the three consecutive nodes (say N1, N2 and N3) work in a group to detect the malicious nodes in the network. If node N1 transmits the data to the intermediate node N2 and then N2 forward it to the next node N3. Node N1 receives the acknowledgement after the successful transmission of data to the desired node N3. After receiving the packets, node N3 will forward the acknowledgement to the source node and the acknowledgement should be authenticated[14] and encrypted by using ECC algorithm. The proposed system assumes that the public and private keys for every node are generated and it is distributed in advance. ECC algorithm [16][17] is used to improve the network security and provides better performance when compared to other cryptographic algorithms such as DSA and RSA.

When the source node receives the acknowledgement, it decrypts the acknowledgement by using the same ECC algorithm and verifies the received acknowledgement time with the expected acknowledgement time. If there is a time out or the received acknowledgement is beyond from the expected transmission time, then there may be possibility of malicious activity. The malicious node may not forward the packet to its next hop. There may be a chance for dropping packets [9]. To overcome the packet dropping attack, the identified malicious node will be blocked from the path and it will be replaced by another energy efficient node. The transmission will be continued by forwarding the packets from the temporarily stored buffer.

4.1.1 Packet Dropping

If there is no malicious activity in the three consecutive nodes,

- Node N1 forwards the packet to node N2.
- Node N2 transmits that received packets to the destination node N3.
- Node N1 receives the acknowledgement about the transmission.

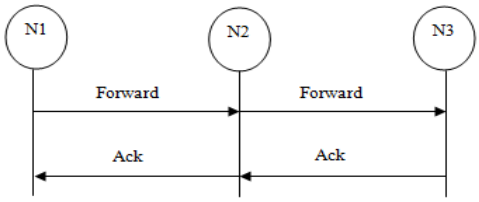

Figure 4.1.1 Packet Transmission

4.1.2 Alternate Node for transmission

If there is a malicious activity,

- Neglect the malicious node or block the malicious node from the route.
- Choose the alternate energy efficient node for transmission which replaces the malicious node.
- Forwards the temporarily stored packets from the buffer.

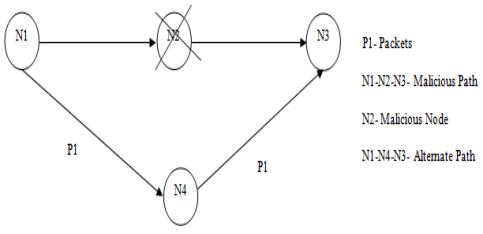

Figure 4.1.2 Alternate node for Transmission

By selecting alternate node instead of choosing alternate path will minimize the energy and overhead for transmission.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1.3 Receiver Collision Avoidance

If two nodes forward the packets to the particular node at the identical time of transmission, then there will be a collision incidence. To resolve this issue the following steps are proposed. That is in this scheme, if the node N3 receives the request from node N2 and N4 at the same time, then node N3 should give the precedence to the requested nodes N2 and N4. The node N3 set the precedence according to the path length and packet size holds to be transmitted. If both the nodes having same path length and packet size, then the precedence should be set according to the energy of nodes for transmission. The node which is having low energy for transmission will get the first preference to transmit the packets.

- The high precedence node will get the first chance to transmit the packets.
- After completion of high precedence node transmission, lower precedence node starts the transmission of packets.
- Compare the acknowledgement time with the expected time of acknowledgement.

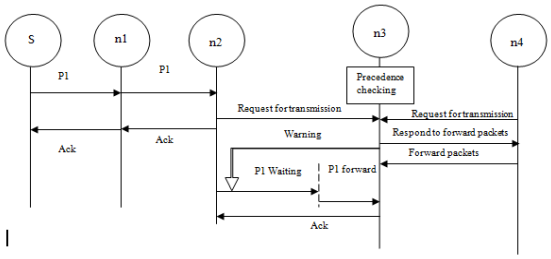

Figure 4.1.3 Receiver Collision Avoidance

4.1.4 Evades False Misbehavior Report Generation

There may be a False Misbehavior Report generation through receiver collision prevention. When there is an acknowledgement from destination node after the time out then that node will be considered as malicious. Due to the waiting time of the lower precedence nodes, the expected acknowledgement time (T_A) should increase sufficiently and there is a possible to report that innocent nodes as malicious. The waiting time (W_T) increased the expected acknowledgement time T_A as $T_E = T_A + W_T$. The proposed system suspends the false misbehavior report generation through the following verification steps.

- Initially the expected acknowledgement time is considered as T_A.
- When the sender node receives the acknowledgement about the transmission it should verifies that whether the ACK > T_A or not.
- If ACK > T_A then verify if $\mathbf{T_A > T_E}$, else report status about the forwarded packets.
- If $\mathbf{T_A > T_E}$ is true then generates the misbehavior report about the malicious node and blocks that node by choosing alternate path for transmission; else confirmed that node is not a malicious and report status about the transmitted packets.

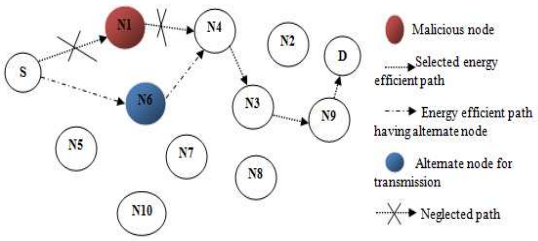

Figure 4.1.4 Block the Malicious Node from the path

The figure 4.1.4 represents the alternate node selection in case of malicious node presents in the network. The misbehaving node N1 which appears in the network may falsely report that the innocent nodes as malicious. The misbehaving node is blocked from the path and another one node N6 will be selected and it replace the malicious node N1 from the selected path for transmission.

5. PERFORMANCE EVALUATION

This section describes the simulation methodology and environment and the proposed system is compared with the existing IDS Watchdog[6], TWOACK[7], AACK[8] and EAACK[9] schemes.

5.1. Simulation Methodologies

To understand the performance of the proposed scheme, three scenarios are considered to simulate different types of misbehaviors or attacks.

Scenario 1: This scenario is used to test the performance of the proposed system against packet-dropping attack in presence of malicious nodes. Comparison results obtained from the performance of the proposed scheme against Watchdog, TWOACK, AACK and EAACK (RSA and DSA).

Scenario 2: This scenario is used to test the performance of the proposed system against false misbehavior report. In this case malicious nodes always drop packets that they receive and send back false misbehavior report. Comparison results

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

obtained from the performance of the proposed scheme against Watchdog, TWOACK, AACK and EAACK (RSA and DSA).

Scenario 3: This scenario is used to test the performance of the proposed system when the attackers are smart enough to forge acknowledgment packets. Comparison results obtained from the performance of the proposed scheme against TWOACK, AACK and EAACK (RSA and DSA).

5.2. Simulation Configuration

The proposed system is simulated using Network Simulator NS 2.29 environment. In order to better compare simulation results with other research works, the default scenario settings in NS 2.29 is adopted. The default configuration of 50 nodes in a flat space with a size of 800 x800 m is considered for simulation. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2.29. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. The detailed simulation parameters are listed in the table 5.1.

Table.5.1. Simulation Parameters

Parameters	Value
Simulation Area	800 m X 800 m
Simulation Time	1000 seconds
Number of Nodes	50
Mobility Model	Random Waypoint Model
Maximum Speed	20 meters/sec
Traffic Type	UDP / CBR
Packet Size	512 B

To compare the proposed system, the following performance metrics are considered.

Packet Delivery Ratio: It is defined as the ratio of number of packets received by the receiver to the number of packets delivered by the transmitter i.e. *no of received packets / no of transmitted packets*.

Routing overhead (RO): It is the ratio of the amount of routing related transmissions (RREQ, RREP,RERR etc.,) to data transmissions in a simulation.

During the simulation, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, a RERR message is sent to the source node in DSR routing protocol. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

5.3. Performance Evaluation and comparison

***Simulation Results – Scenario 1*:** Figure 5.3.1 illustrates the routing overhead of proposed scheme against other schemes such as Watchdog, TWOACK, AACK and EAACK in the presence of packet dropping attack. The other approaches use alternate path for transmission when malicious node is encountered in the network path but the proposed approach does not use the alternate path for transmission. Thus the routing overhead is minimized because there is no need for another route request and route response for transmission which reduces the routing overhead. The results show that the proposed scheme achieves higher performance than the previous intrusion detection approaches.

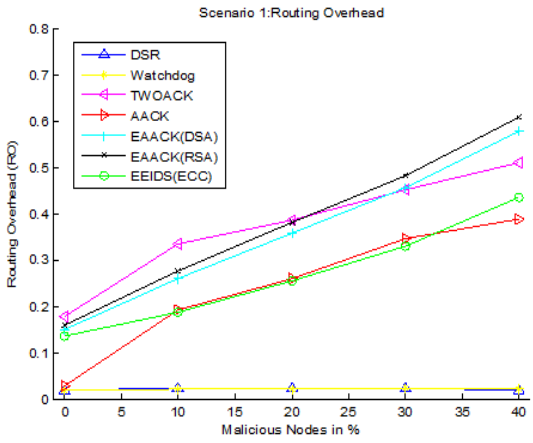

Figure 5.3.1: *Routing overhead vs. malicious node*

Figure 5.3.2 demonstrates the packet delivery ratio in the presence of packet dropping scenario. It

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

shows that the proposed scheme reaches the higher level than the other approaches in case of packet delivery ratio. When there is a dropping of packets the buffer used to forward the packets and it avoids the retransmission of packets which saves the energy and improves the packet delivery ratio. There may be a slight possibility for dropping packets, because the network replaces the malicious node and if there any dropping of packets, then the buffer can forward the packets to the desired node.

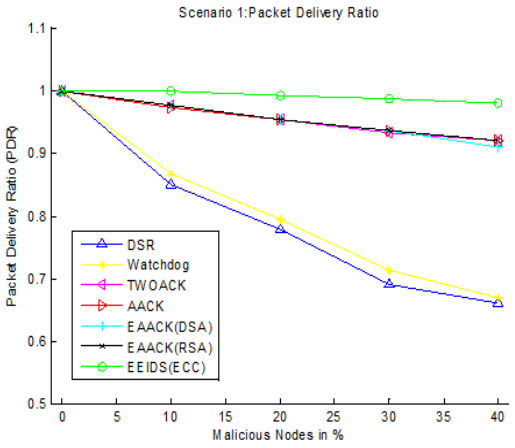

Figure 5.3.2: *packet delivery ratio vs. malicious node*

Simulation Results – Scenario 2: The False misbehavior report can be generated by the misbehaving nodes to falsely report innocent nodes as malicious nodes. If the acknowledgement is received after the time out period then there may be a malicious activity. When false misbehavior report is generated as a result of malicious nodes, those nodes are blocked from the network and another node should be selected for transmission.

Figure 5.3.3 shows that the proposed approach has the minimum routing overhead in the presence of false misbehavior report compared to other existing intrusion detection approaches.

Figure 5.3.4 illustrates the packet delivery ratio in the presence of false misbehavior report generation by the malicious nodes in the network. Since misbehaving nodes are detected efficiently, the proposed scheme achieve higher packet delivery ratio in this scenario also, when compared to other Intrusion detection approaches.

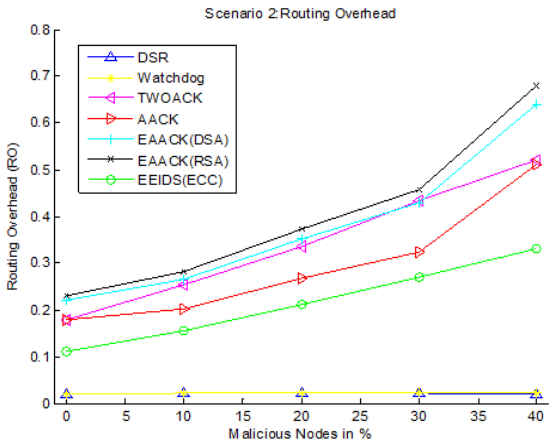

Figure 5.3.3: *Routing overhead vs. malicious node*

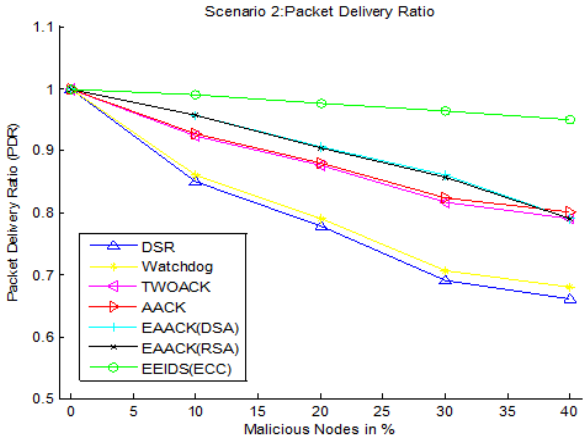

Figure 5.3.4: *packet delivery ratio vs. malicious node*

Simulation Results – Scenario 3: In this scenario the malicious nodes are provided with the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgement packets to its previous node whenever necessary. This is a common method used by the attackers in order to degrade the network performance while still maintaining its reputation.

Figure 5.3.5 and 5.3.6 illustrates the *Packet Delivery Ratio* and routing overhead in the presence of the attackers. Since the malicious nodes are identified efficiently in the proposed approach, packet dropping is minimized. Hence the proposed scheme achieve higher packet delivery ratio when compared to other IDS schemes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

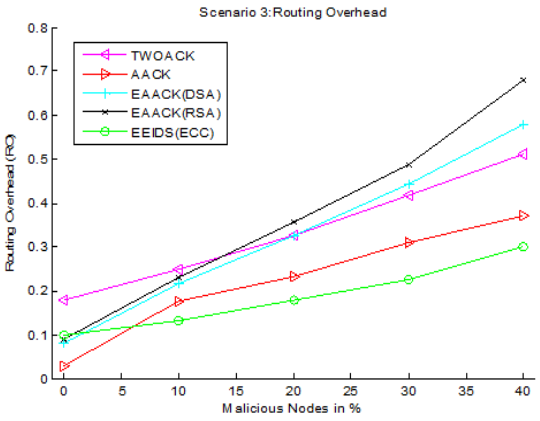

Figure 5.3.5: *Routing overhead vs. malicious node*

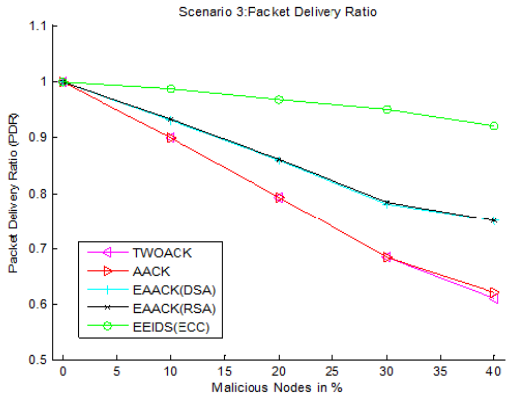

Figure 5.3.6: *packet delivery ratio vs. malicious node*

6. CONCLUSION

Routing attacks are the major hazards towards the security of ad-hoc networks, especially in MANET. The proposed system specially designed for detecting MANET security attacks without affecting the network performances. Elliptic Curve Cryptography (ECC) significantly improves the security when compared to other DSA and RSA cryptographic algorithms in the acknowledgement process. The consideration of three consecutive nodes for packet transmission notably minimizes the routing overhead and improves the network performance. The limited transmission power, packet dropping, receiver collision and false misbehavior report attacks are also circumvented by the proposed scheme. The proposed scheme with ECC detects the malicious node efficiently and provides better results against Watchdog and other previous acknowledgement based IDS in the presence of the issues such as routing overhead, limited transmission power, packet dropping, receiver collision and false misbehavior report. Simulation results were shown that the proposed scheme achieve higher packet delivery ratio than the previous acknowledgement based IDS scheme.

7. REFERENCES

[1]. Vydeki, D. and R.S. Bhuvaneswaran," Effect of Clustering in Designing a Fuzzy Based Hybrid Intrusion Detection System for Mobile Adhoc Networks", Journal of Computer Science, 9 (4): 521-525, 2013.

[2]. Vydeki, D. and R.S. Bhuvaneswaran," Design of Wireless IDS using Adaptive Neuro-Fuzzy Inference System", European Journal of Scientific Research, Vol. 90 No 1, pp.149-156 November, 2012.

[3]. V. Anjana Devi and R. S. Bhuvaneswaran," Agent based Cross Layer Intrusion Detection System for MANET", In the Proceedings of 4th international conference, CNSA 2011 ,July 2011 Springer-Heidelberg (CCIS) volume 196, pp427-440.

[4]. V. Anjana Devi and R. S. Bhuvaneswaran, "Adaptive Association Rule Mining based Cross Layer Intrusion Detection System for MANET", International journal of network security and its applications, Volume 3 , number 5, pp243-256 September 2011

[5]. S. D. Khatawka, U. L. Kulkarni and K. K. Pandyaji, "Detection of Routing Misbehavior in MANETs", International Conference on Computer and Software Modeling IPCSIT volume.14 Singapore, 2011.

[6]. Marti, S., Giuli, T.J., Lai, K., Baker, and M.: Mitigating routing misbehavior in mobile ad-hoc networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Net-working (MobiCom'00) pp. 255–265 (2000)

[7]. Balakrishnan, K., Jing, D., Varshney, and V.K.: TWOACK: preventing selfishness in mobile ad hoc networks. IEEE Wirel. Commun.Netw. Conf.4, 2137–2142 (2005)

[8]. Tarek Sheltami, Anas Al-Roubaiey, Elhadi Shakshuki and Ashraf Mahmoud, "Video

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

transmission enhancement in presence of misbehaving nodes in MANETs", Multimedia Systems (2009) 15:273–282.

[9]. Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013.

[10]. RakeshShrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han, "A Novel Cross Layer Intrusion Detection System in MANET", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[11]. AbrorAbduvaliyev, Sungyoung Lee, Young-Koo Lee, "Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks", International Conference on Electronics and Information Engineering (ICEIE), 2010.

[12]. G. S. Mamatha and Dr. S. C. Sharma, "A New Combination Approach to Secure MANETS against Attacks", International Journal of Wireless & Mobile Networks (IJWMN), Volume.2, No.4, November 2010.

[13]. Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on DEPEDABLE and Secure Computing, 2011.

[14]. S.Jeyashree, "Highly Secure Distributed Authentication and Intrusion Detection with Data Fusion in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[15]. Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications Volume 41– No.21, March 2012.

[16]. F. Amounas and E. H. El Kinani "ECC Encryption and Decryption with a Data Sequence", Applied Mathematical Sciences, Vol. 6, 2012, no. 101, 5039 – 5047.

[17]. Dr. Jean- Yves Chouinard, "Notes on Elliptic curve cryptography", Design of secure Computer Systems CSI4138/CEG4394, September 24, 2002.

[18]. K. S. Sujatha , Vydeki, D. and R.S. Bhuvaneswaran," Design of Genetic Algorithm based IDS for MANET", in the proceedings of IEEE conference (ICRTIT) 2012.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

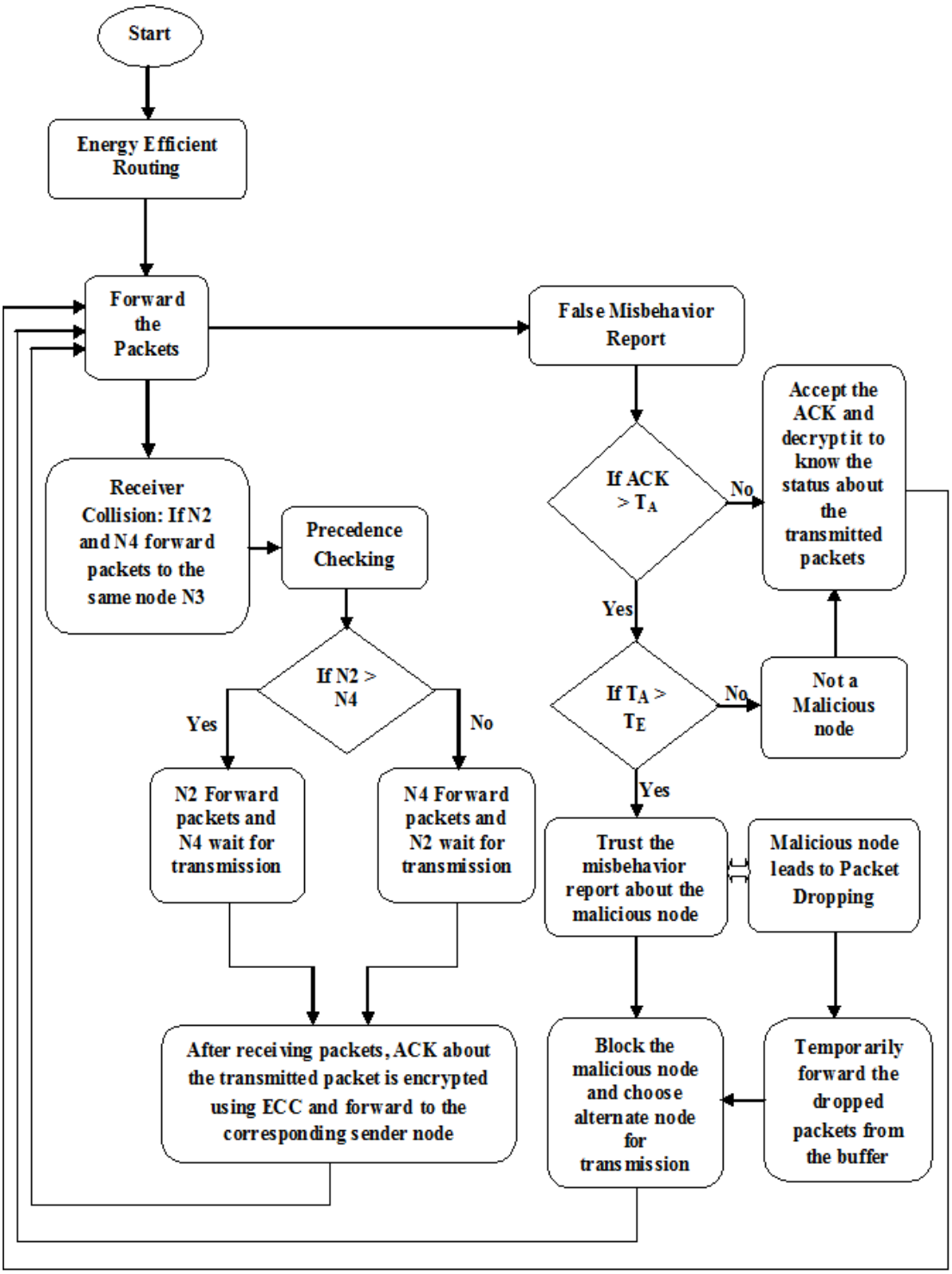

Figure 4.1 System Flow Model