International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

A Trust and Intrusion Detection based Secure Routing Algorithm for Mobile Ad-Hoc Networks

K. Thangaramya[1], S. Mohammed Nuhuman[2]
[1]*Student of Engineering,* [2]*Assistant Professor, Department of CSE, National College of Engineering, TamilNadu*

***Abstract*— The use of Mobile Ad hoc Networks (MANETs) has increased in recent years mainly due to their advantages and their broad applications. MANETs are dynamic peer-to-peer networks that consist of a collection of mobile nodes. These nodes perform multi-hop information transfer without requiring a predefined infrastructure. Recently, Intrusion Detection System (IDS) plays a major role in the security of MANETs. Moreover, IDSs are an effective way to detect various types of attacks in networks thereby securing the MANETs. An effective Intrusion Detection System requires high accuracy and detection rate as well as low false alarm rate. In this paper, we propose a new intrusion detection system called Intelligent Enhanced Adaptive ACKnowledgment(IEAACK) specially designed for MANETs. The proposed system introduces a new digital signature to prevent the attacker from forging acknowledgment packets. Moreover, we propose a trust prediction model to secure the network effectively. The model can evaluate the trustworthiness of nodes, based on the historical behaviours of nodes. Finally, a multi-path secured routing scheme is used in this work. The experimental results obtained in this work show high detection rates and reduce the false alarm rate.**

***Keywords*— Intrusion Detection System, Mobile Ad hoc Networks, Secure Routing, Trustworthiness.**

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) consist of mobile nodes that work independently without an infrastructure. They are useful in application areas like disaster management, emergency and rescue operations where it is not possible to have well-defined infrastructure. Moreover, MANETs are characterized by its great flexibility and mobility of nodes. However, MANET's inherent vulnerability increases its security risks. Though MANET is dynamic and cooperative in nature, it needs efficient and effective security mechanisms to safeguard the mobile nodes.

Intrusion detection and prevention are primary mechanisms of security since they attempt to reduce possible intrusions. Intrusion detection using classification algorithms effectively discriminates "normal" behavior from "abnormal" behavior. Therefore, intrusion detection and prevention systems can be used as a secondary mechanism of defense in any wireless environment and MANETs so that it can be a part of the reliable communication in MANETs [2].

Conventional intrusion detection and prevention strategies, such as firewalls, access control schemes and cryptographic methods used in the past for providing security to the data communicated through the ad hoc networks have failed to prove themselves for effectively protecting networks and systems from increasingly sophisticated attacks. In such a scenario, Intrusion Detection Systems (IDS) turn out to be the proper solution to tackle these issues and have become an essential component in security systems since they are used to detect the threats before they induce widespread damage. The design and construction of IDS has many challenges including data collection, data pre-processing, and identification of malicious nodes, reporting and response. Among these entities, identification of malicious nodes is an important activity which is highly indispensable [2].

Trust is an important security measure that represents a MANET participant's anticipation of the other nodes behavior when assessing the risk involved in further communication. Here, the participant is usually called the truster, and other nodes are called the trustee. The trust relationship usually builds on the basis of the trusters past interaction experiences and recommendations of other related to the trustee, measured using a score called reputation. Trust management in MANETs is necessary when communicating with new nodes without any preceding interactions. This is helpful for providing secure communication [10].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

In this paper, we propose a new intrusion detection system named Intelligent Enhanced Adaptive ACKnowledgment(IEAACK) specially designed for MANETs. In this system a new digital signature scheme is employed to prevent the attacker from forging the acknowledgment packets. Moreover, we propose a trust prediction model which can evaluate the trustworthiness of nodes using the current and historical behaviours of nodes. Finally, a multi-path secured routing scheme is also used to improve the network security.

Remainder of this paper organized as follows: Section 2 describes the related works on trust based intrusion detection. Section 3 explains the proposed trust based intrusion detection algorithm. Section 4 provides the implementation details of the proposed algorithm. Section 5 discusses the results of the proposed system. Section 6 gives the conclusion and some possible future direction of this direction.

II. Related Work

Liu et al [5] proposed a new technique called 2ACK scheme for the detection of routing misbehavior in MANETs. This 2ACK scheme serves as an add-on technique for routing schemes to detect routing misbehavior and to prevent their adverse effect. In 2ACK scheme, two-hop acknowledgment packets are sent in the opposite direction of the routing path. Due to this, even if the nodes participate in the route discovery and maintenance processes, it may refuse to forward data packets when they suspect the packets. This approach is used to reduce the additional routing overhead. This is due to the fact that only a fraction of the received data packets are acknowledged in the 2ACK scheme. Sheltami et al [6] proposed a new method for the detection of misbehaving nodes in MANET. Their system examines the effect of packet dropping attacks on video transmission over MANETs. The node uses the ACK scheme which sends an acknowledgment to ensure the delivery of the data packets between each three consecutive nodes in the path. The authors call it is an adaptive acknowledgment scheme (AACK) since it has the ability to detect misbehaved nodes and avoid them in other transmissions.

Jemili et al [4] proposed a multipath extension of a hierarchical routing, which constructs link-disjoint paths and selects less congested and correlated paths for an efficient data transfer and resources use. The performance of the multipath algorithm illustrated by them using simulation results. Moreover, this multipath extension is more effective under various traffic loads in terms of packet delivery ratio and control overhead. Ha Dang et al [3] investigated the distributed clustering scheme and proposed a cluster-based routing protocol for Delay-Tolerant Mobile Networks. An exponentially weighted moving average scheme is employed by them for on-line updating nodal contact probability, were its mean converges to the true contact probability. Moreover, it achieves higher delivery ratio and significantly lower overhead and end-to-end delay compared with its non-clustering counterpart. Aiguo et al [1] proposed a novel cluster-based trust model for ad hoc networks and an inter-cluster recommendation trust method has been introduced by the authors. In their model, a network is divided into clusters with one special node in each cluster. It establishes the trust relationship for internal clusters dynamically based on the results obtained in previous transactions. Uncertainty problem with nodes coming and going in spontaneous ad hoc environments solved with this model.

A secure node disjoint multipath routing protocol for wireless sensor networks was proposed by Shiva Murthy et al [7]. In their work, the data packets are transmitted in a secure manner by using the digital signature algorithm. Moreover, their model is compared with an ad hoc on-demand multipath distance vector routing protocol. From the results shown, it is observed that their model shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multipath distance vector routing. Weiqi Dai et al [9] proposed a novel solution called dubbed Assured Digital Signing (ADS), to enhance the data trustworthiness vouched by digital signatures. In order to minimize the modifications to the Trusted Computing Base (TCB), ADS simultaneously takes advantage of trusted computing and virtualization technologies. Specifically, ADS allows a signature verifier to examine not only a signature's cryptographic validity but also its system security validity.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Hence, the private signing key and the signing function are secure, despite the powerful attack that the signing application program and the general-purpose Operating System (OS) kernel are malicious.

III. System Model

The architecture of the system proposed in this paper is shown in Fig. 1. It consists of three major modules namely IEAACK Module, Trust Prediction Module and Secure Routing module.

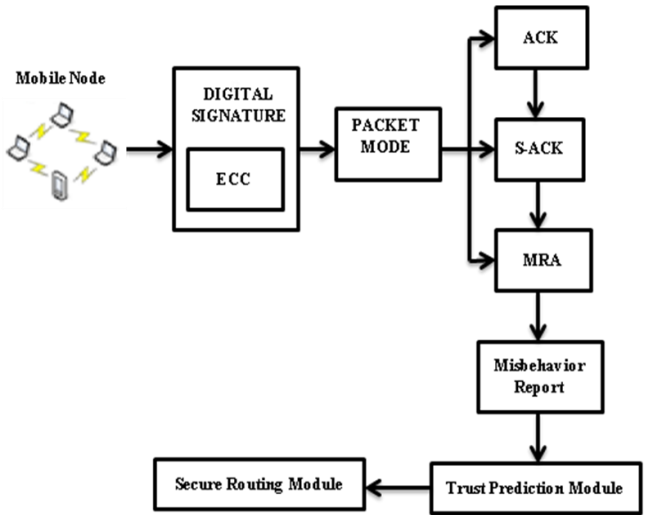

Fig. 1. System Architecture

A. Intelligent EAACK Module

This module contains three sub sections namely Digital Signature generation, Acknowledgement method and Misbehavior Report. Digital Signature is generated an elliptic curve cryptography algorithm based on Diffie Hellman Algorithm. Acknowledgement method is used to send the acknowledgements in different types such as ACK, Secure ACK and Misbehavior Report Authentication based on the decision making agent suggestion. The Misbehavior Report is used to finalize the misbehavior report based on MRA.

B. Trust Prediction Module

In Trust prediction module, we used the ad hoc on-demand trusted-path distance vector (AOTDV) algorithm [5] to compute the node trust for the decision making.

C. Secure Routing Module

In this module, we used a multipath routing protocol called ad hoc on-demand multipath distance vector (AOMDV) routing protocol [5] for improving the security.

IV. Proposed Work

In this paper, we propose a new intrusion detection system called an Intelligent Enhanced Adaptive ACKnowledgment (IEAACK) specially designed for MANETs. The proposed system introduces a new digital signature which is used an elliptic curve cryptography algorithm to prevent the attacker from forging acknowledgment packets. Moreover, we used a trust prediction model for enhancing the security. The model evaluates the trustworthiness of nodes using the ad hoc on-demand trusted-path distance vector (AOTDV) algorithm [5]. Finally, a multi-path secured routing scheme called AOMDV [5] is also used which performs routing by using route discovery, trust values and using an IDS.

A. IEAACK Algorithm

Input : Information (Data)
Output: Misbehavior Nodes Report

Step 1: Choose all the nodes present in the MANET.
Step 2: Monitor the node activity which are present the scenario and create security agents.
Step 3: Apply the Elliptic Curve Cryptography algorithm based on Diffie Hellman Scheme for encryption for detecting the forging acknowledgement.
Step 4: The security agent decides the acknowledgement type.
  a) If the transmissions are end-to-end process then
     Store the ACKnowledgement status
  b) If the transmissions are between three consecutive nodes
     then
     Store the Secure ACKnowledgement status.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

c) The MRA finalizes the misbehaving nodes based on the Acknowledgement status of the every nodes.

Step 5: Generate the misbehaving nodes report by MRA.

B. Ad-hoc On-demand Trusted-path Distance Vector (AOTDV) algorithm

We used an effective trust based algorithm called Ad-hoc On-demand Trusted path Distance Vector (AOTDV) [5] to predict the nodes which are present in the network scenario and not present in the MRA misbehaving report.

C. Ad-hoc On-demand Multipath Distance Vector (AOMDV) Routing Protocol

In this paper, we used an effective multipath routing protocol called ad hoc on-demand multipath distance vector (AOMDV) routing protocol [5] for improving the security in which route discovery considers trust as well as intrusion behaviour during routing.

V. Result And Discussion

For simulating our proposed routing protocol, we used NS2 (Version 2.34.1) [8]. The AODV routing protocol is used for all simulation and the simulation parameters. The topology of the MANET depends on the pause time and mobility speed and also it changes its topology frequently when pause time is less and mobility speed is more. We compared the performance of EAACK in presence of malicious node and the performance of the proposed technique without the presence of malicious node.

TABLE I
DELAY ANALYSIS FOR EAACK AND IEAACK

Algorithms	No. of Packets Sent					
	6000	8000	10000	12000	14000	16000
Delay in EAACK (ms)	0.7	1.8	2.9	3.2	3.4	3.7
Delay in IEAACK (ms)	0.695	1.79	2.89	3.12	3.27	3.54

Table I shows the delay analysis that makes a comparison between the EAACK and the proposed IEAACK. From this table, it can be observed that elimination of the malicious nodes reduces the delay.

Fig. 2 shows the better performance of IEAACK with respect to malicious node presence in terms of packet delivery ratio. From figure 2, it can be observed that the performance of packet delivery ratio is improved considerably in the IEAACK of this work when it is compared with EAACK.

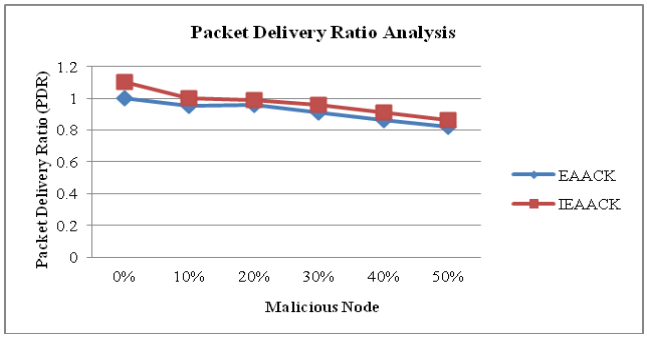

Fig. 2. Comparative Packet Delivery Ratio Analyses between IEAACK and EAACK

Fig. 3 shows the better performance of the proposed system with respect to malicious node presence in terms of packet delivery ratio. From figure 3, it can be observed that the performance of packet delivery ratio is improved considerably in the IEAACK of this work when it is compared with EAACK.

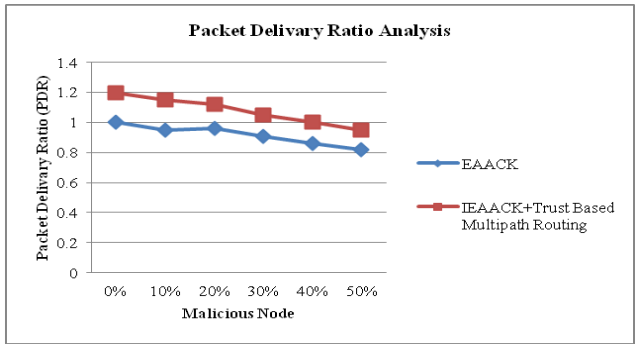

Fig. 3. Packet Delivery Ratio Analysis

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Fig. 4 shows the better performance of the proposed system with respect to the malicious nodes presence in the network scenario. From figure 4, it can be observed that the performance of detection accuracy has been improved reasonably in the proposed system in this work when it is compared with EAACK and IEAACK.

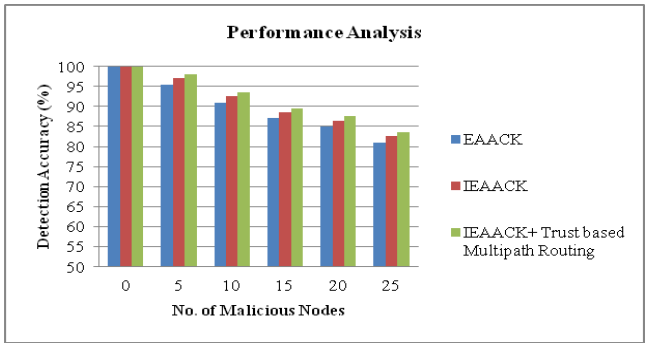

Fig. 4. Performance Analysis

Fig. 5 shows the throughput analysis of the proposed system in comparison with EAACK and IEAACK in presence of less number of malicious nodes in network. Figure 5 shows the better performance of proposed system with respect to mobility in the presence of large number of malicious nodes.

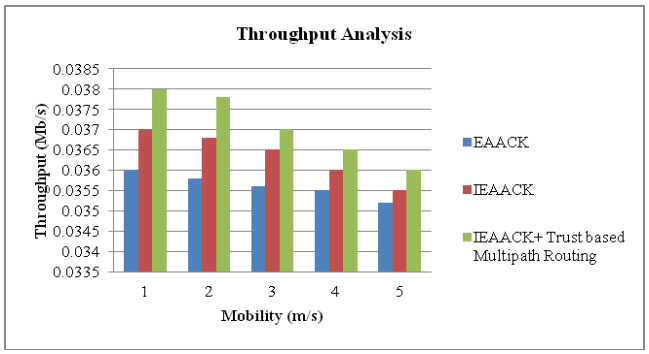

Fig.5. Throughput Analysis

From Fig. 5, it can be observed that the performance of throughput analysis is improved reasonably in the proposed system when it is compared with the proposed IEAACK and EAACK. All these improvements are due to the use of intelligent agents, trust modeling and IDS.

VI. CONCLUSION

In this paper, we propose a new intrusion detection system named Intelligent Enhanced Adaptive ACKnowledgment (IEAACK) specially designed for MANETs. The proposed system introduces a new digital signature algorithm to prevent the attacker from forging acknowledgment packets. Moreover, we propose a trust prediction model that evaluates the trustworthiness of nodes, based on the historical behaviours of nodes. Finally, a multi-path secured routing scheme also proposed and implemented. Further works in this direction could be the use of fuzzy logic for trust enhancement and to improve the decision process.

REFERENCES

[1] Aiguo Chen, Guoai Xu, Yixian Yang, "A Cluster-Based Trust Model for Mobile Ad Hoc Networks", 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2008.

[2] Feng Li, Ju Wu, "Uncertainty Modeling and Reduction in MANETs", IEEE Transactions on Mobile Computing, Vol.9, No.7, pp. 1035-1048, 2010.

[3] Ha Dang , Hongyi Wu , "Clustering and cluster-based routing protocol for delay-tolerant mobile networks", IEEE Transactions on Wireless Communications, Vol. 9, No.6, pp. 1874-1881, 2010.

[4] Jemili, I., Chaabouni, N., Belghith, A., Mosbah, M., "A Multipath Layered Cluster Based Routing for Ad Hoc Networks", 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-5, 2012.

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

[6] Sheltami, T., Al-Roubaiey, A., Shakshuki, E. and Mahmoud, A. "Video transmission enhancement in presence of misbehaving nodes in MANETs", Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[7] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 12, No. 10, pp 2941-2949, Oct. 2012.

[8] The Network Simulator (NS2), http://www.isi.edu/nsnam/ns/

[9] Weiqi Dai, T. Paul Parker, Hai Jin, and Shouhuai Xu, "Enhancing Data Trustworthiness via Assured Digital Signing", IEEE Trans. Dependable and Secure Computing, Vol. 9, No. 6, pp. 838-851, Nov/Dec. 2012.

[10] X.Li Z. Jia P. Zhang R. Zhang H. Wang, "Trust-based on-demand Multipath Routing in Mobile Ad hoc Networks", IET Information Security, Vol. 4, No. 4, pp. 212–232, 2010.