IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 19-24
www.iosrjournals.org

An Approach Towards Handling Packet Loss Ratio Using Eaack (Iddsa) Algorithm

S.Gomathi[1]

[1](*Department of Computer Science ,Sankara College of Science and Commerce, Coimbatore, India)*

Abstract: *Mobile ad hoc Network (MANET) is a collection of mobile nodes equipped with every wireless-transmitter and receiver that communicate with one another via bi-directional wireless links either directly or indirectly. A replacement intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. Throughout this thesis, a replacement intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) is specially designed for MANETs and ID based mostly digital Signature scheme is projected. The results will demonstrate positive performances against Watchdog, TWOACK and AACK within the cases of receiver collision, restricted transmission power and false misbehavior report, packet delivery Ratio. This EAACK IDentity-based Digital Signature Algorithm (IDDSA) scheme and Packet Loss Ratio is calculated in the proposed work and compared with existing methods for better performance.*

Key words: *rSerPool, Watchdog, TWOACK, AACK, EAACK, IDDSA, Packet Loss Ratio (PLR)*

I. Introduction

Mobile ad hoc Networks (MANETs) are of increasing interest for various sets of applications. Instead of using any centralized infrastructure, nodes in MANET cooperate with one another to provide networking during their movements. Such capability is essential for some special scenarios like battlefield or emergency field work wherever preexisting or centralized communication infrastructures are not offered. MANET on the battlefield will offer various services to support different missions such as enemy situation, battlefield map, etc. Such applications place increasing demands on reliable transport and persistent sessions. Successful realization of those services faces tremendous challenges not only owing to a harsh communication setting due to the factors of node mobility, radio fading, and interfering, but also due to enemies' attacks.

Reliable server pooling (rSerPool) is an approach that provides the reliability of services by introducing redundancy in the number of servers available to a client. The architecture and protocols for the operation and management of rSerPool are being developed by Internet Engineering Task Force (IETF) [1] to support highly reliability-demanding applications on Internet. The advantages of rSerPool, especially the fail-over merit, make it very attractive in tactical MANETs. However, the characteristics of
MANETs indicate that the rSerPool protocols for Internet applications have to be tailored largely to fit MANET applications.

In this paper, we propose and implement a new intrusion-detection system named Adaptive Accommodative Acknowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while doesn't\'t greatly affect the network performances. Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection[4].

II. Background Study

Friend based Ad hoc routing using Challenges to Establish Security (FACES) is an algorithm to provide secure routing in ad hoc mobile networks. We propose this scheme that has been drawn from a network of friends in real life scenarios. [3].

In this paper, we study leader election in the presence of selfish nodes for intrusion detection in mobile ad hoc networks (MANETs). To address the issue of selfish nodes, we present a solution based on mechanism design theory. The solution provides nodes with incentives in the form of reputations to encourage nodes in honestly participating in the election process [4].

A novel route discovery algorithm called endairA was proposed, together. In this paper, we show that the security proof for the route discovery algorithm endairA is flawed, and this algorithm is vulnerable to a hidden channel attack. We also analyze the security framework that was used for route discovery and argue that composability is an essential feature for ubiquitous applications. We conclude by discussing some of the major security challenges for route discovery in MANETs[5].

III. Problem Definition

The proposed EAACK is designed to tackle three of the six weaknesses of Watchdog mechanism, namely, false misbehavior, limited transmission power, and receiver collision.

As a result of the open medium and remote distribution of typical MANETs, attackers will simply capture and compromise one or two nodes to realize this false misbehaviour report attack[2]. TWOACK and AACK solve two of those three weaknesses, namely, receiver collision and limited transmission power. During this analysis work, our goal is to propose new IDS specially designed for MANETs, that solves not only receiver collision and limited transmission power however additionally the false misbehavior problem. we extend our analysis to adopt a digital signature scheme during the packet transmission method. As in all acknowledgment-based IDSs, it is important to make sure the integrity and authenticity of all acknowledgment packets.

IV. Scheme Description

Our proposed EAACK (IDDSA) scheme is in detail. The approach described in this analysis paper is based on our previous work [6], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to stop the attacker from formation acknowledgment packets. EAACK is consisted of three major elements, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In EAACK, we use a pair of b of the 6-b to flag differing types of packets. We assume that the link between every node within the network is bi-directional. Moreover, for every communication method, both the source node and also the destination node are not malicious. Unless specified, all acknowledgment packets described during this research are required to be digitally signed by its sender and verified by its receiver

4.1 ID BASED DIGITAL SIGNATURE SCHEME FOR SECURITY

In this work, the zero-knowledge based identification scheme by Popescu [6] is transformed into a digital signature scheme through conversion of one-way hash function. There are two characteristics in one way hash function (OWHF).The output is of a fixed length instead of the variable length of the input; also, the length of the signed message can be reduced, so that the chosen message attack as defined by ElGamal [4] can be prevented. But in OWHF, the disadvantage is that the security level degrades proportionally. This paper revisits the construction of Universal One-Way Hash Functions (UOWHFs) from any one-way function.

4.1.1 Universal a method hash functions (UOWHF)

A UOWHF is a keyed hash perform with the subsequent property: if associate degree adversary chooses a message x, then a key k is chosen at random and given to the adversary, it\'s laborious for the adversary to seek out a different message $x' \neq x$ such that $H_k(x) = H_k(x')$. A UOWHF that hashes fixed-length messages, then style a technique for composing these compression functions so on hash arbitrary messages [7].

V. Performance Evaluation

In this section, we focus on simulation environment and methodology, comparing performances through simulation result with Watchdog mechanism, TWOACK, EAACK (IDDSA) schemes.

5.1. Simulation Methodologies

To better investigate the performance of EAACK under differing kinds of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks simulated a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to check the performance of IDSs against 2 weaknesses of Watchdog, namely, receiver collision and limited transmission power.

5.2. Simulation Configurations

Our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The performances of our proposed theme tend to still adopt the following three performance metrics.

1) Packet delivery ratio (PDR): defines the magnitude relation of the amount of packets received by the destination node to the amount of packets sent by the supply node.

2) Routing overhead (RO): artificial language defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

3) Packet Loss Ratio (PLR): Packet loss happens once or additional packets of knowledge traveling across a network fail to achieve their destination. Packet loss is distinguished mutually of the 3 main error; the opposite two being bit error and spurious packets caused due to noise.

Mathis formula builds on a number of assumptions, and here we report only the ones that are more relevant to our model:

1. SACKs are implemented, so that multiple losses in a RTT are indication of a single congestion event;
2. The receiver window is big enough and the sender has always data to send;
3. The connection never times-out and always recovers from a loss using fast retransmit and fast recovery;
4. The connection is long enough to reach steady state;
5. The RTT is constant over the path.

Note that, if assumptions 1-3 are not met, the result is a reduced goodput, while, if assumption 4 is not met, the result may be a higher goodput. This happens when slow start overestimates the available capacity, and congestion avoidance starts from an operating point far from the actual equilibrium. (i.e.)

$$goodput = \frac{MSS.C}{RTT.\sqrt{PLR}} \qquad (1)$$

Where:

a) good put is given by the size of delivered data over the delivery completion time;
b) MSS is the maximum segment size, that is typically 1460 bytes per packet;
c) C is a constant that incorporates the loss model and the acknowledgment strategy. When the loss model is random and TCP uses delayed ACKs, the value of this constant is 0.93;
d) RTT is the round trip time;
e) PLR is the number of congestion signals per acknowledged packet.

In our model, assume MSS = 1460,C = 0.93, and we derive the packet loss rate (PLR) from (1) to obtain:

$$PLR = \left(\frac{MSS.C}{goodput.RTT}\right)^2 \qquad (2)$$

During the simulation, upon receiving this RREQ message, every neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives identical RREQ message quite once, it ignores it. If a failed node is detected, that generally indicates a broken link in flat routing protocols like DSR, a RERR message is distributed to the supply node. Once 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 within the RREQ message.

5.3 **Performance Evaluation**

Our simulation results are,

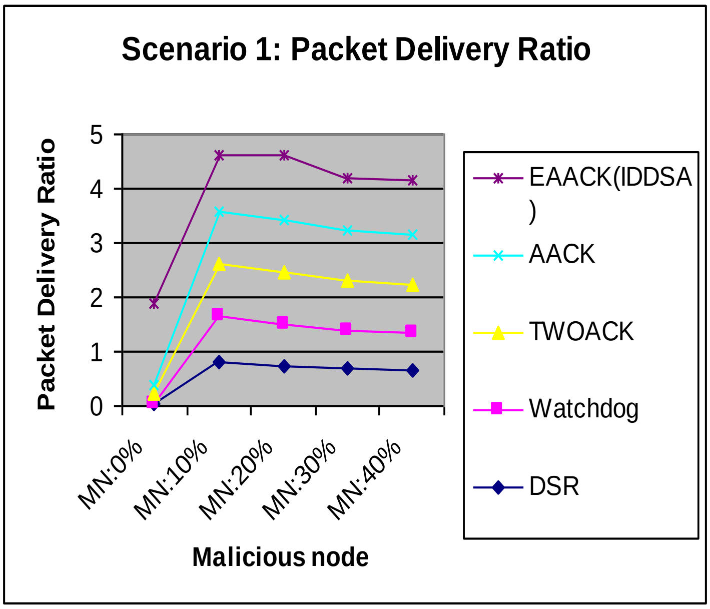

Figure.1: Simulation results for scenario 1—PDR.

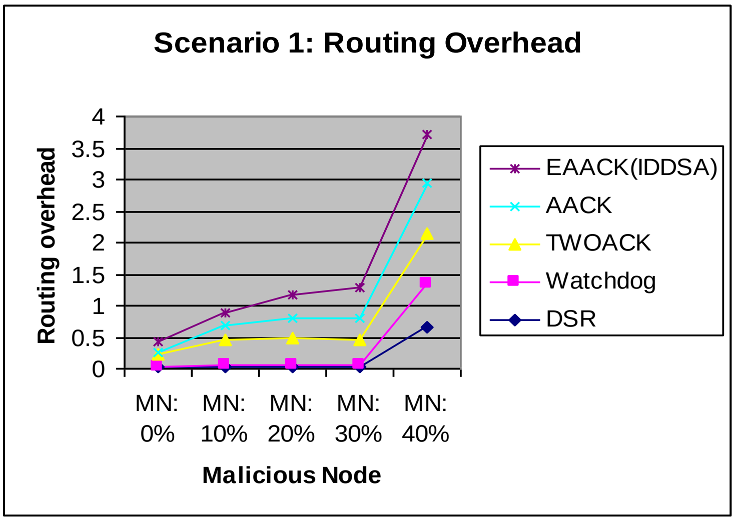

Figure.2: Simulation results for scenario 1—RO.

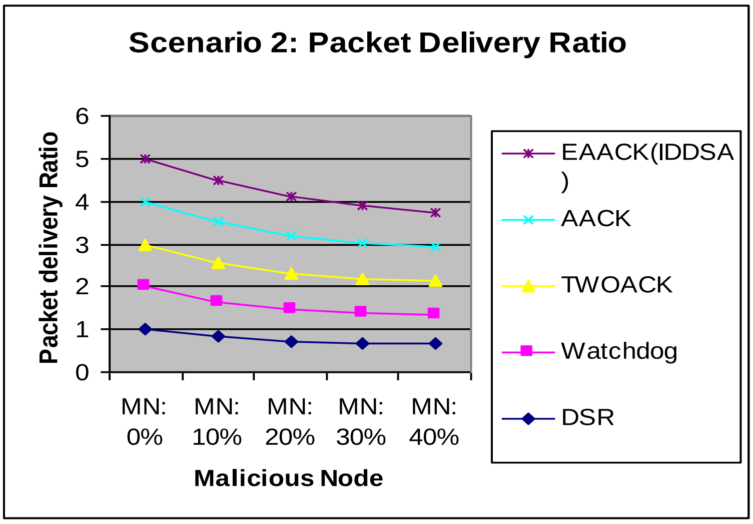

Figure.3: Simulation results for scenario 2—PDR.

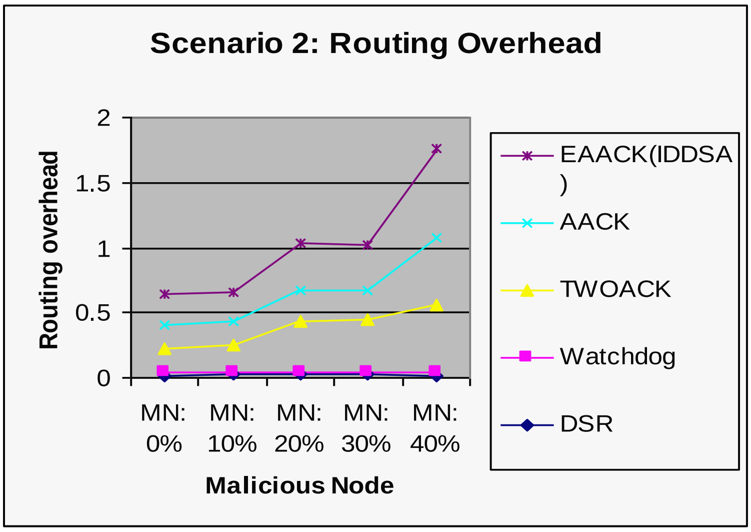

Figure. 4: Simulation results for scenario 2—RO.

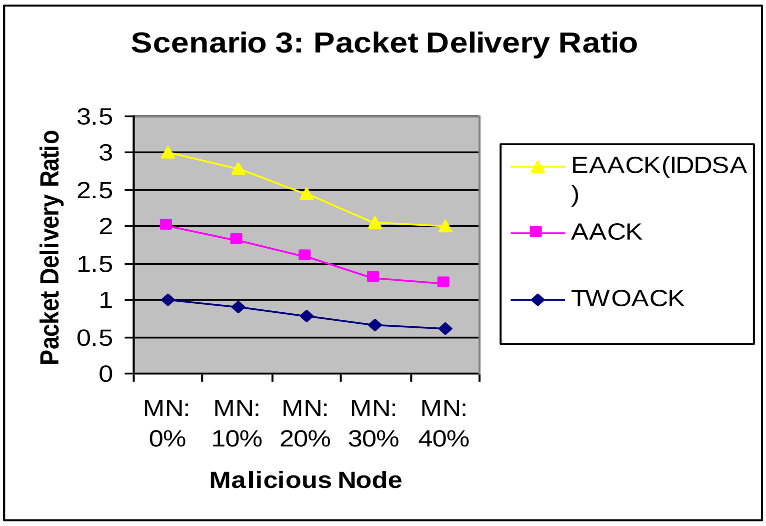

Figure.5: Simulation results for scenario 3—RO.

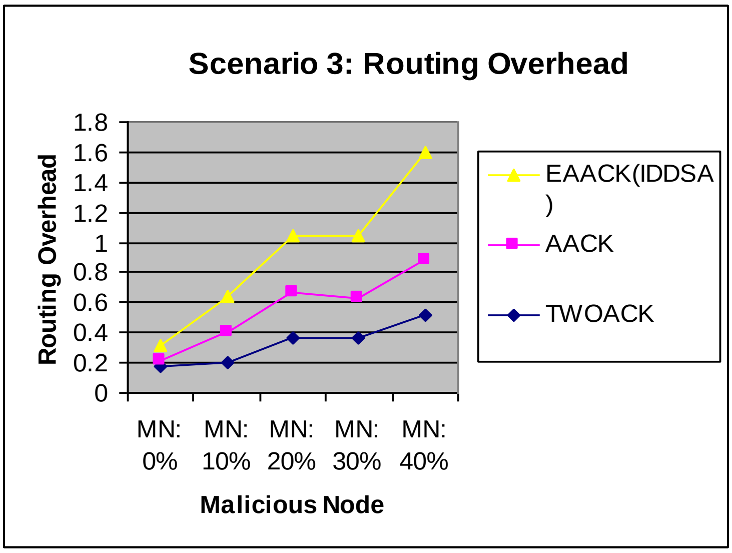

Fig. 6: Simulation results for scenario 3—RO.

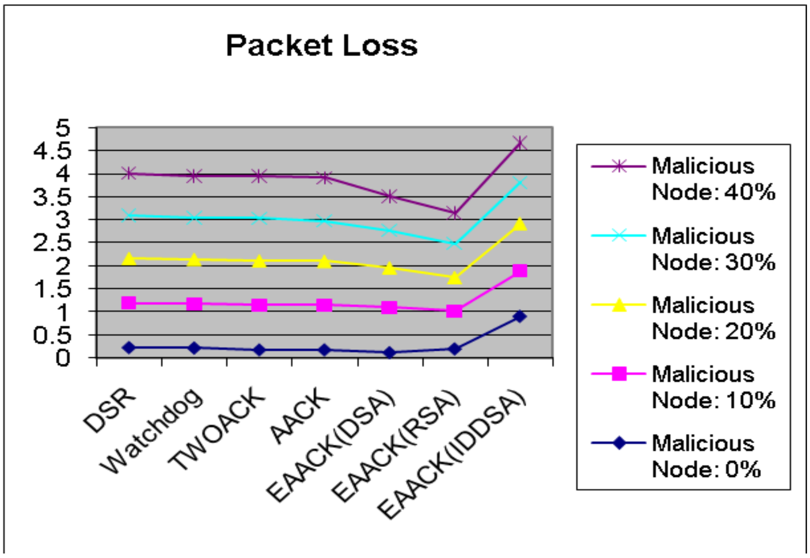

Figure.7: Simulation results for scenario 1—PL.

VI. Conclusion

This approach uses the Packet-dropping attack has always been a significant threat to the security in MANETs. This analysis paper, we have proposed a novel IDS named EAACK(IDDSA) protocol. The results demonstrated positive performances against Watchdog mechanism, TWOACK, and AACK in the cases of receiver collision, limited transmission power, false misbehavior report and packet loss. Compared to this proposed work and PLR can be estimated by a simple measure of goodput and RTT.

Reference

[1]. Architecture for reliable server pooling [Online]. Available: www.ietf.org/ids.by.wg/rserpool.html

[2]. Burmester, M., de Medeiros, B., “On the Security of Route Discovery in MANETs”, Mobile Computing, IEEE Transactions on (Volume:8 , Issue: 9) Page(s): 1180 – 1188.

[3]. Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P., Dhurandher, P., “FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems”, Systems Journal, IEEE 2011 (Volume:5 , Issue: 2), Page(s): 176 – 188.

[4]. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory 31 (4) (1985) 469–472.

[5]. Mohammed, N., Otrok, H., Lingyu Wang, Debbabi, M., Bhattacharya, P., “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET”, Dependable and Secure Computing, IEEE Transactions on 2011, Page(s): 89 – 103.

[6]. C. Popescu, An identification scheme based on the elliptic curve discrete logarithm problem, The 4th International Conference on High-Performance Computing in the Asia-Pacific Region, vol. 2, 2000, pp. 624–625.

[7]. S.Gomathi, N.Sudha Bhuvaneswari, “Study on Secured Intrusion-Detection System with Enhanced Adaptive Acknowledgement for MANET using Universal Hash Function”, International Journal of Mobile Communication and Technologies.