International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-7)

Research Article

July 2013

Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System

Prof. Anusha.K[1], Rajyalakshmi G.V[2]
School of Information Technology and Engineering,
VIT University, Vellore – 632014, India

Abstract:

A Mobile Ad-hoc network (MANET) is an infrastructure-less network consisting of self-configuring mobile nodes associated by wireless links. Every single node works both as a transmitter and a receiver. Nodes correspond directly with each other when they are both within the same communication range. If not, they rely on their neighbors to relay messages. Furthermore, MANETs are highly vulnerable for passive and active attacks because of their rapidly changing topology, open medium and lack of centralized monitoring. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the advanced improvements in technology and cut in hardware costs, we on look the current tendency of expanding in use of MANETs into industrial applications. To amend to such trend, we strongly consider that it is vital to strengthen its potential security issues. For this, we propose and implement an intrusion-detection system named Improved Intrusion Detection System (IIDS) for MANETs. Compared to contemporary approaches, IIDS demonstrates higher malicious-behavior-detection rates under certain circumstances while not greatly affecting the network performances.

Keywords: Security, Mobile ad-hoc network, Intrusion detection system, Secure Adaptive Acknowledgement.

I. Introduction

Wireless networking is the platform for working with the current technology used widely in many more applications. Mobile ad hoc networks (MANETs) combine wireless communication with high level of node mobility. Restricted range wireless communication and high level node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure so that needs are continuously met [1]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in serious mission applications like military conflict or emergency recovery. Nominal configuration and quick deployment make MANET ready to be used in emergency conditions where an infrastructure is unavailable or infeasible to install in scenarios like natural or military conflicts, human-induced disasters, and medical emergency situations [2]. Owing to these unique characteristics, MANET is becoming more broadly implemented in the industry. However, considering the fact that MANET is popular among critical applications, network security is of fundamental importance. Unfortunately, remote distribution of MANET and the open medium make it vulnerable to different types of attacks. For example, owing to the node's lack of physical protection, malicious attackers can easily confine and compromise nodes to achieve attacks. In particular, allowing for the fact that most routing protocols in MANETs assume that every node in the network behaves considerately with other nodes and presumably not malicious [3], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Also, because of MANET's distributed architecture and changing topology, a conventional centralized monitoring technique is no longer feasible in MANETs. In such case, it is vital to develop an intrusion detection system (IDS) specially designed for MANETs.

A. Intrusion Detection System

Intrusion detection is very important aspect of defending the cyber infrastructure from attackers or hackers. Intrusion prevention technique such as filtering router policies and firewalls fail to stop such kind of attacks. Therefore, no matter how well a system is protected, intrusion still occurs and so they should be detected. Intrusion detection systems are becoming significant part of security and the computer system. An intrusion detection system is used to detect many types of malicious behaviors of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET knows how to detect the attackers as soon as they enter the network, we will be able to completely remove the potential damages caused by compromised nodes at the first time. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. The present research mechanism has focused on designing Intrusion Detection Systems (IDS) to monitor and analyze system events for detecting network resource misuse in a MANET.

II. Literature survey

Marti et al. [4] proposed a scheme named Watchdog that aims to enhance the throughput of network with the presence of malicious nodes. In reality, the Watchdog scheme consisted of two different parts, namely, Watchdog and

Pathrater. Watchdog serves as an ID for MANETs and it is responsible for detecting the malicious node misbehaviors in the network. Watchdog detects the malicious misbehaviors by prominently listening to its next hop's broadcast. If a Watchdog node overhears that its next node fails to forward the packet within a definite period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node informs it as misbehaving node. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many research studies and implementations have proved that the Watchdog scheme is efficient. Besides, compared to some other schemes, Watchdog is competent of detecting malicious nodes rather than links in the network. These advantages have made the Watchdog scheme a popular choice in the field. Nevertheless, as pointed out by Marti et al. [4], the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following ie. Ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report.

With respect to the weaknesses of the Watchdog scheme, many researchers proposed novel approaches to solve these issues. TWOACK proposed by Liu et al. [5] is one of the most significant approaches among them. On the contrary to many other schemes in detecting malicious nodes, TWOACK is neither an enhancement nor a Watchdog-based scheme to detect malicious nodes. Aiming to resolve the receiver collision and limited transmission power harms of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node down the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. The same process applies to every three consecutive nodes down the rest of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power harms posed by Watchdog. Though, the acknowledgment process required in every packet transmission process added a major amount of unwanted network routing overhead. Owing to the limited battery power nature of MANETs, such unneeded transmission process can easily degrade the life span of the entire network. The main disadvantage of TWOACK technique is Routing overhead.

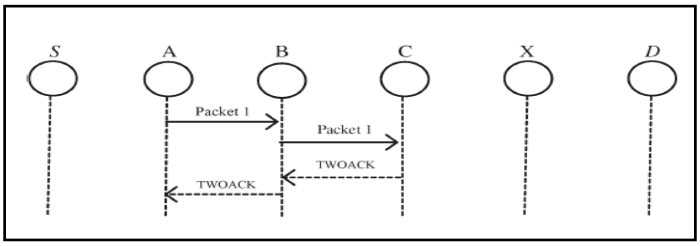


Fig. 1 TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

A. *Adaptive Acknowledgement (AACK)*

Based on TWOACK, Sheltami et al. [6] proposed a new scheme that is called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be measured as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK considerably reduces network overhead while still capable of maintaining or even surpassing the same network throughput during data transmission. The end-to-end acknowledgment scheme in ACK is shown in Fig. 3. In the ACK scheme the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. In this network all the intermediate nodes simply forward this packet to the next nodes. When the destination node D receives Packet 1, it is vital to send back an ACK acknowledgment packet to the source node S down the reverse order of the same route. Within a predefined time, if the source node S receives this ACK acknowledgment packet from the destination node, then the packet transmission from node S to node D is successful. Or else, the source node S will switch to TACK scheme by sending out a TACK packet.
SHAKSHUKI et al.: EAACK—A SECURE INTRUSION-DETECTION SYSTEM FOR MANETs 1091

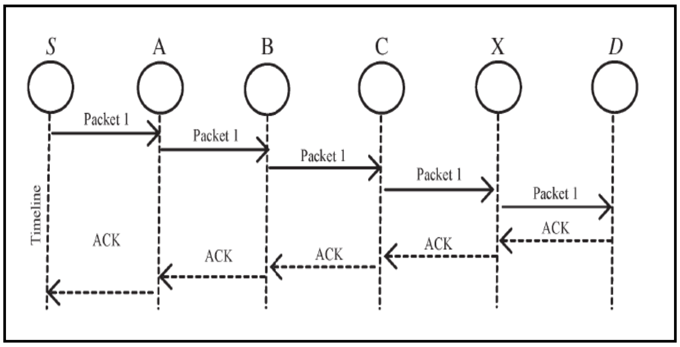


Fig. 2 AACK scheme: The destination node is required to send acknowledgment packets to the source node.

III. Methodologies

It is highly vital to guarantee that the data packets are valid and authenticated in the existing system. In order to ensure the integrity of the IDS, IIDS requires data packets to be encrypted before they are sent out and verified until they are accepted. To address the problem of extra resources required due to the introduction of security in MANETs we adopt a security in our proposed scheme namely Improved IDS (IIDS) to achieve the goal of finding the most optimal solution for using security in MANETs.

IIDS uses AODV routing protocol to find the shortest path in the network to reach destination. Then it encrypts the data packet with hash key and send to the destination. The destination decrypts the data and check the hash value for data integrity. If the route has attacker nodes and if the sender does not receive acknowledgement packets then the packets will be sent in the new route. If any node wants to send packet to neighboring node then first source node generate the packet and send to the neighboring node. The sent packet is sent to acknowledge system in which we AACK with security. After that it send packet according to mode and detect the intruder in the system, If intruder or misbehaving node is detected then alert will be triggered by the same node that detect the misbehaving node. When a node detect malicious node it will inform the source node by sending an acknowledgement, which is a small packet that is generated by the routing protocol and extract the route from source route of corresponding data packet and the packet will be sent in a new route.

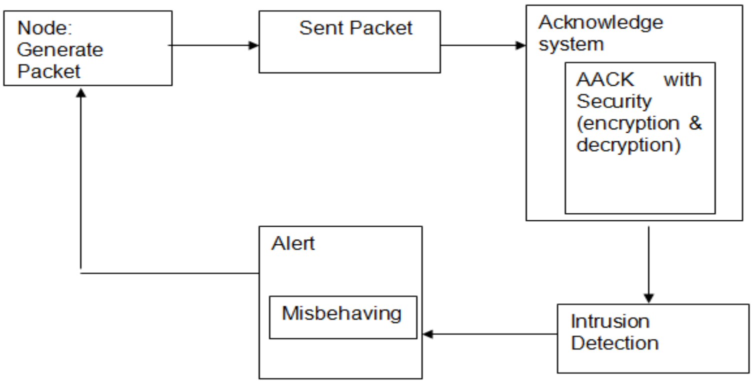


Fig.3 Architecture Design

B. Security

Security based on hash function [7] has always been an integral part of cryptography. Using a simple hash algorithm, hash value from a string of plain text can be generated. The hash value will be attached to packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded. In either case, an acknowledgement packet will be sent back to sender to inform of the status of the packet.

C. Encryption and decryption functions

For encryption and decryption feature we implement CESAR cipher with pre-shared key of 3. These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text to three positions. Any encryption/decryption algorithm with symmetric key can be implemented here.

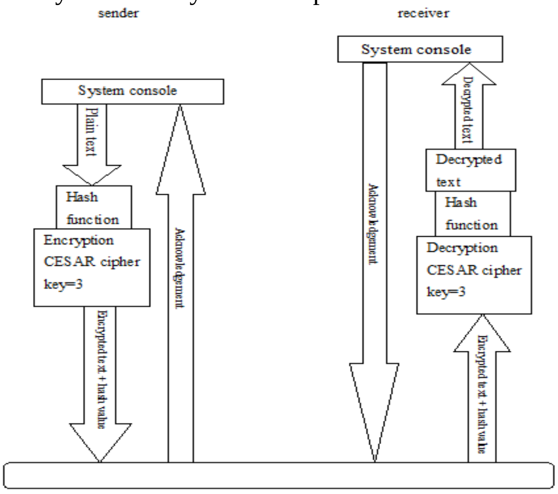


Fig.4 Logical Design of encryption and decryption system

IV. Implementation

As discussed before, IIDS is an acknowledgment-based IDS. AACK is an acknowledgment-based detection scheme. It relies on acknowledgment packets to sense misbehaviors in the network. Thus, it is extremely important to make sure that all acknowledgment packets in IIDS are untainted and authentic. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be defenseless. With regard to this serious concern, we incorporated security in our proposed scheme. In order to make sure the integrity of the IDS, IIDS requires AACK acknowledgment packets to be encrypted before they are sent out and verified until they are accepted. In order to reduce the extra resources required due to the implementation of digital signature in MANETs, CEASAR encryption and decryption scheme has been incorporated in the present work since the ultimate goal is to find the most advantageous solution for using security in MANETs.

A. *Implementation of Security Packet*

Marc Greis's tutorial shows how to build a new packet protocol to NS-2 (Fig. 4.2). The new packet class is created in the folder ns2.30. After that, the new packet name has to be registered to the packet.h. Then the make file has to be modified so that the new class is compiled. At the TCL layer, the new packet must be acknowledged by adding the name and default packet size value to the ns-default.tcl file. Finally, we have to create an entry for the new packet in the ns-packet.tcl file. After recompile the ns-2, we can use the new packet for our simulation.

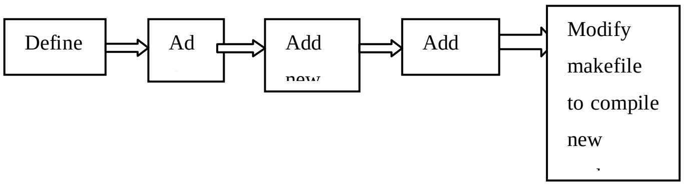


Fig.5 Flow chart of adding new protocol to NS-2

We propose to make a new packet class carrying data. The parameters of the class comprise encryption and decryption algorithms, it generate messages digest functions for integrity. Cesar cipher is chosen to demo encrypt and decrypt algorithms. The message digest generator is the hash function in C++.

B. *Hash function*

A cryptographic hash function is a hash function, in which an algorithm takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) modification to the data will (with very high probability) modify the hash value. The data that has to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digests.

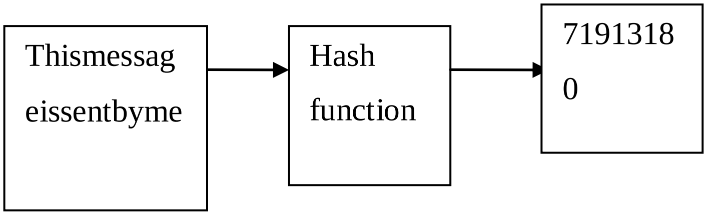


Fig. 6 Hash function process

C. Encryption and Decryption function

The encryption can be represented with modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly with,

$$D_n(x) = (x - n) \mod 26.$$

V. Simulation model

Our simulation contains 30 nodes scattered on a 800X800 meter flat space for data transfer. This space makes the maximum hops to be 3. The physical layer and 802.11 MAC layer are included in the wireless extensions of NS2 . Table 1.1 shows the other simulation parameters. UDP traffic with constant bit rate (CBR) is used with packet size of 512 bytes and data rate of 4 packets per second. Each data point was obtained by running the simulation 10 times with different seed numbers and taking the average value of the results. The misbehaving nodes population varies from 0% to 40% with 10% increments. The smart attackers' number is set to a constant percentage of 40% from the total number of misbehaving nodes.

TABLE 5.1
Simulation Parameters

Parameter	Value
Number of nodes	30 nodes
Simulation area	800 meter x800 meter
Simulation time	10 sec
Mobility model	Fixed Mobility
Speed range	Uniformly distributed (1-20) meter/second
Traffic type	CBR
Packet size	512 bytes
Routing Protocol	AODV

I. Performance metrics

These following metrics are used to evaluate the performance of IIDS for existing and proposed technique which are defined as follows:

Packet delivery ratio (PDR)

It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

$$PDR = \frac{\sum Received\ packets\ at\ destinations}{\sum Sent\ packets\ by\ sources}$$

Routing Overhead (RoH)

This is the ratio of routing related packets in bytes (RREQ, RREP, RERR, AACK,) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgments, alarms and switching over head is included.

$$RoH = \frac{\sum Routing\ transmissions}{\sum Data\ \ transmissions + \sum Routing\ transmissions}$$

Average end-to-end delay (AED)

The average end-to-end delay for all successfully received packets at the destination. It is calculated for each data packet b subtracting the sending time of the packet from the received time at final destination. Then the average represents the AED.

$$AED = \frac{\sum_1^N (T_{Rceived} - T_{Sent})}{N}$$

Where N is number of successfully received packets

Throughput:

The average rate of successful message is delivery over a communication channel.

Scenario 1 : Packet Delivery Ratio

TABLE 5.2
Packet Delivery Ratio

	Malicious Nodes: 0%	**Malicious Nodes:10%**	**Malicious Nodes :20%**	**Malicious Nodes :30%**	**Malicious Nodes :40%**
AODV	1	0.334	0.334	0.334	0.334
AACK	1	0.938	0.8	0.73	0.7
IIDS	1	0.9	0.92	0.92	0.9

Scenario 1 : Average end-to-end delay

TABLE 5.3
Average end-to-end delay

	Malicious Nodes: 0%	**Malicious Nodes:10%**	**Malicious Nodes:20%**	**Malicious Nodes:30%**	**Malicious Nodes:40%**
AODV	0.141	0.025	0.025	0.025	0.025
AACK	0.161	0.161	0.401	0.324	0.38
IIDS	0.3	0.22	0.410	0.55	0.55

Scenario 1 : Routing overhead

TABLE 5.3
Routing Overhead

	Malicious Nodes: 0%	**Malicious Nodes:10%**	**Malicious Nodes:20%**	**Malicious Nodes:30%**	**Malicious Nodes:40%**
AODV	0.33	0.33	0.33	0.33	0.33
AACK	0.351	0.351	0.846	0.967	1.004
IIDS	0.895	0.462	1.002	0.979	0.979

Scenario 1 : Throughput

TABLE 5.4
Throughput

	Malicious Nodes: 0%	**Malicious Nodes:10 %**	**Malicious Nodes: 20%**	**Malicious Nodes: 30%**	**Malicious Nodes: 40%**
AODV	2733	1370	1370	1370	1370
AACK	2734	2734	2134	1962	1961
IIDS	2543	2281	2531	2464	2464

Scenario 1: Packet Delivery Ratio

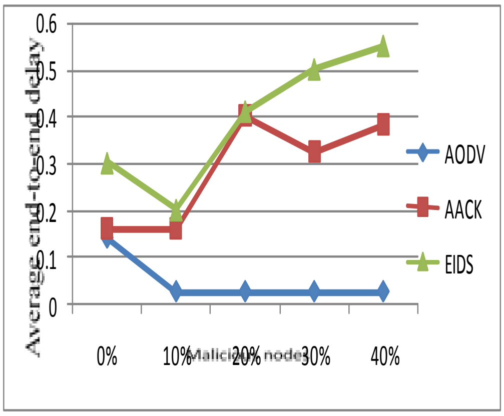


Fig. 7 Packet delivery ratio

Packet-dropping attack has always been a major threat to the security in MANETs. And thus IIDS can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.

Scenario 1: Average end-to-end delay

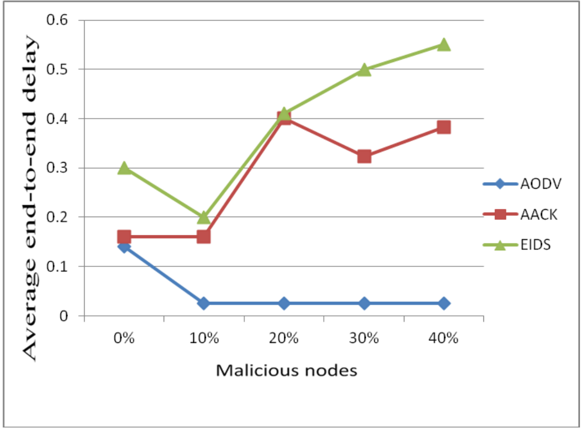


Fig. 8 Average end-to-end delay

Scenario 1: Routing overhead

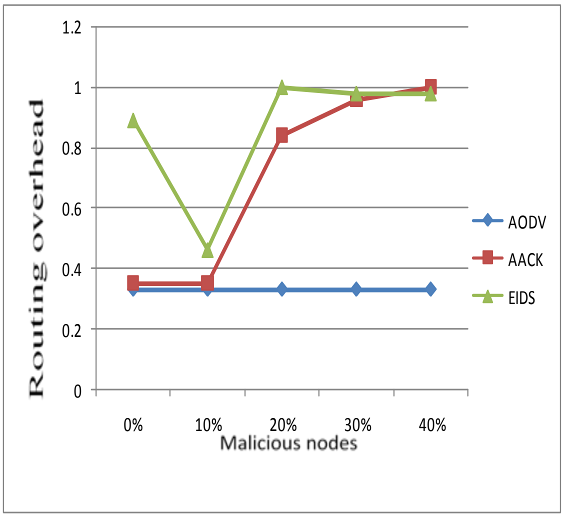


Fig. 9 Routing overhead

Scenario 1: Throughput

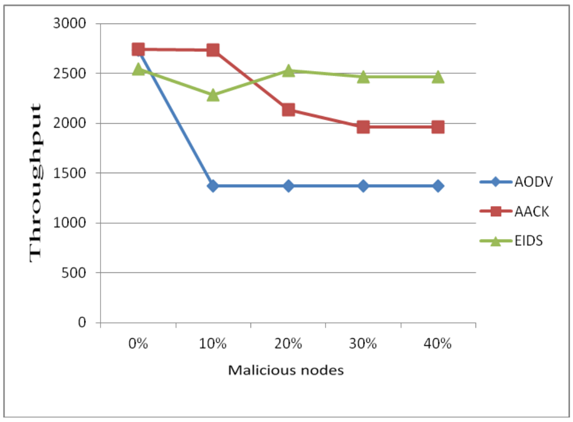
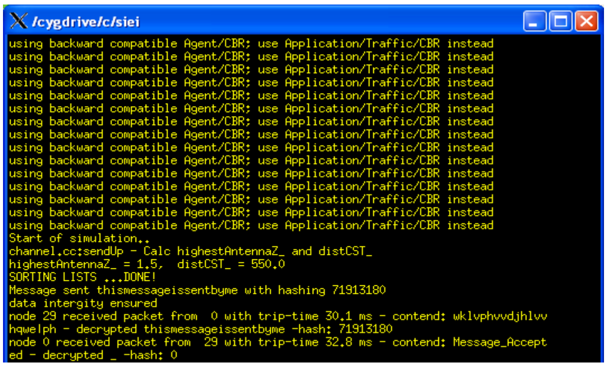


Fig. 10 Throughput

Scenario 2: IIDS

Where as in IIDS the data which are being sent through the attacker node are not modified since they are secure i.e they are encrypted before they are sent and if the attack is so smart that they can decrypt, then it will take time .In which,if the sender do not receive the acknowledgement, then that node will be detected as misbehaving node. Now the sender selects other path to send the data. The following is the snapshot of the result for the sending of secure data through the compromised node.

Snapshot of the IIDS output



```
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
Start of simulation..
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Message sent thismessageissentbyme with hashing 71913180
data intergity ensured
node 29 received packet from  0 with trip-time 30.1 ms - contend: wklvphvvdjhlvv
hqwelph - decrypted thismessageissentbyme -hash: 71913180
node 0 received packet from  29 with trip-time 32.8 ms - contend: Message_Accept
ed - decrypted _ -hash: 0
```

Fig.11 Secure data transfer

Encrypted data with hash key sent from source to destination and the receiver node decrypts the data with hash key and checks data integrity.

VI. Conclusion & future work

Packet-dropping attack has always been a major risk to the security in MANETs. In the present work we have proposed an Intrusion Detection System namely Improved Intrusion Detection System for MANETs and compared it against other mechanisms in different scenarios through simulations. The results demonstrated optimistic performances against AACK in the cases of receiver collision, false misbehavior report and limited transmission power. Furthermore, in an effort to prevent the attackers from initiating forged data attacks, we extended our work to incorporate security in our proposed scheme. Although it generates more Routing Overhead in the present scheme as demonstrated for some cases, it can vastly advance the network's Packet Delivery Ratio, when the attackers are smart enough to forge acknowledgment packets. We believe that this tradeoff is valuable when network security is the top priority.

To increase the merits of the present work, we do have plans to investigate the following issues in our future research:

1) Possibilities of implementing hybrid cryptography techniques to further reduce the network overhead caused by security.

2) Observe the possibilities of adopting a key exchange mechanism in order to remove the requirement of pre distributed keys.

References

[1] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," *Journal of Computer Science* ., vol. 3, no. 8, pp. 574–582, 2007.

[2] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. *IEEE Int. Conf. Commun., Glasgow, Scotland*, Jun. 24–28, 2007, pp. 1154–1159.

[3] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. *Int. Conf. Mobile Comput*. Netw., Boston, MA, 2000, pp. 255–265.

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

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