Universal Journal of Communications and Network 2(7): 107-117, 2014 http://www.hrpub.org
DOI: 10.13189/ujcn.2014.020701

Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK) Intrusion Detection System

Baseem Adnan AL-Twajre[1,2,*] , Wilson Jeberson[3]

[1]University of Babylon, college of Engineering, Iraq
[2]Department of CSE, SHIATS-Allahabad, India
[3]Department of Computer Science & IT, SHIATS-Allahabad, India

Copyright © 2014 Horizon Research Publishing All rights reserved.

Abstract A mobile Ad-hoc network (MANET) is a wireless network that does not rely on any fixed infrastructure (i.e., routing facilities, such as wired networks and access points), and whose nodes must coordinate among themselves to determine connectivity and routing. The traditional way of protecting networks is not directly applicable to MANETs. Many conventional security solutions are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANETs use might be expected. Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. So, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. To provide high security for information on MANETs, Intrusion Detection Systems (especially that based on acknowledgment packets) used different types of cryptographic algorithms to protect the acknowledgment packets from attacks of intruder. These cryptographic algorithms are required to provide data security and user's authenticity. In this paper we proposed an intrusion-detection model to protect MANETs from attacks named Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK) based on acknowledgment packets. In order to ensure the integrity and high level of security of the proposed model, acknowledgment packets encrypted and digitally signed by its sender before they are sent out and verified by its receiver until they are accepted, for this purpose we use hybrid cryptography Technique. This hybrid cryptography Technique has been used to detect hacking on the acknowledgment packets in intrusion detection systems like RSA hacking problem that appears in other pervious system. We used two algorithms to implement our Hybrid Cryptography technique, Advanced Encryption Standard (AES) algorithm and RSA algorithm. The two algorithms are cooperated to give more security to acknowledgment packets. The proposed model has been compared with other popular mechanisms like watchdog, Two Acknowledgment (Two-ACK), Adaptive Acknowledgment (AACK) and Enhanced Adapted Acknowledgment (EAACK) through simulation by Network Simulator NS 2.34. To evaluate the performance of IDS for existing and proposed technique we estimated the values of three performance metrics Packet delivery factor (PDF), Routing Overhead (OH) and Average end-to-end delay (D) in many scenarios. Compared to contemporary approaches, our proposed model demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords Mobile Ad-hoc Networks (MANETs), Intrusion-Detection Systems (IDSs), Hybrid Cryptography Enhanced Adaptive Acknowledgement (HCEAACK)

General Terms IDS architecture, AES Algorithm, RSA Algorithm, Hybrid cryptography IDS, Malicious nodes

1. Introduction

Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. Mobile Ad-hoc Networks (MANETs) solves this problem by allowing intermediate parties to relay data transmissions.

Mobile Ad-hoc networks (MANETs) combine wireless

communication with a high degree of node mobility. Limited range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met[1],[2].This is achieved by dividing MANET into two types of networks, namely, single-hop and multi hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range [3], [4], [5]. MANETs have been proposed for use in many areas such as rescue operations, tactical operations, environmental monitoring, conferences, and the like [6].

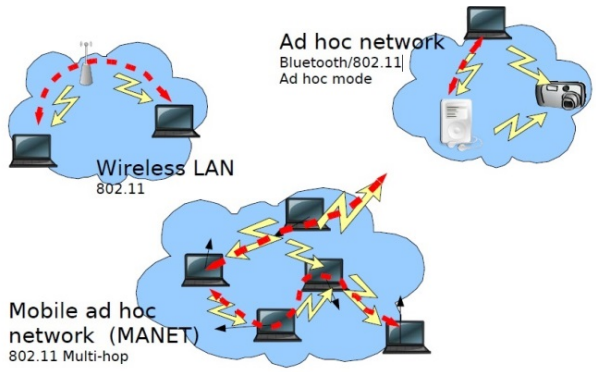

Figure 1. Wireless Networks [12]

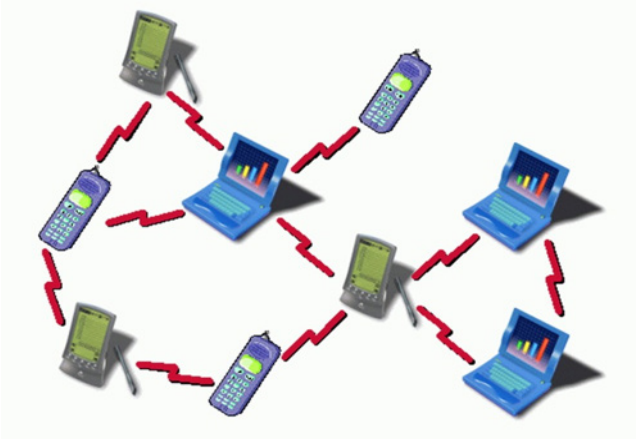

Figure 2. Mobile Ad-hoc Network (MANET).

A mobile Ad-hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each node MANET must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. 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],[2].The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices introduces new security risks [7], [8]. As part of rational risk management we must be able to identify these risks and take appropriate action. In the last few years security problems in MANETs have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion detection and response. As a result, intrusion detection is an indispensable part of security for MANETs. So it is vital to develop an efficient and effective intrusion detection system (IDS) for MANETs. Many research efforts have been devoted to such research topic [1],[6], [10],[11], [12], [13],[14], [15], [16], [17],[18],[19].

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. 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.

2. Background

In this section, we mainly describe four existing approaches for IDS namely, Watchdog [20], TWOACK [12], Adaptive Acknowledgment (AACK) [21], and EAACK [19]:

2.1. Watchdog

It is very popular and highly efficient IDS for improving the throughput of network with the presence of malicious nodes. These IDS can be classified into two methods such as Watchdog and Pathrater. It is responsible for discovering malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by listening to its next hop's transmission in the network. If a Watchdog IDS overhears that its next node fails to forward the packet within a certain

period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

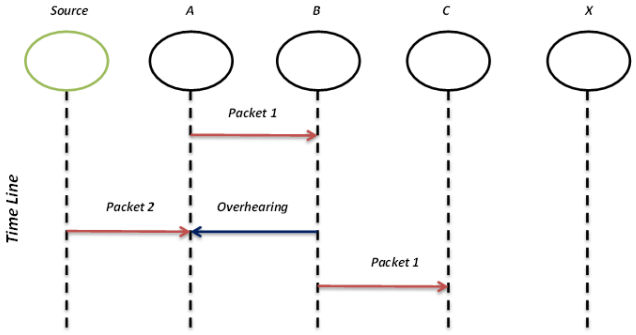

Figure 3. Ambiguous collisions

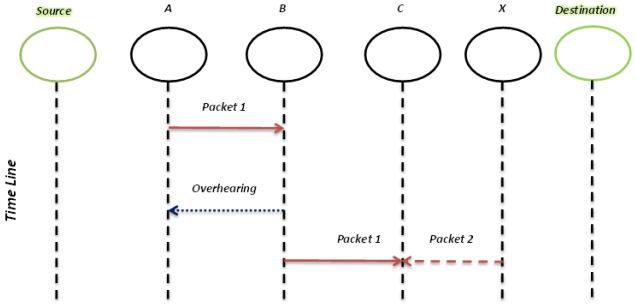

Figure 4. Receiver collision both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

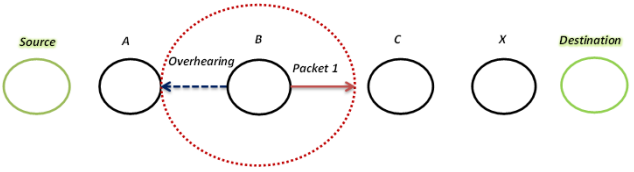

Figure 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

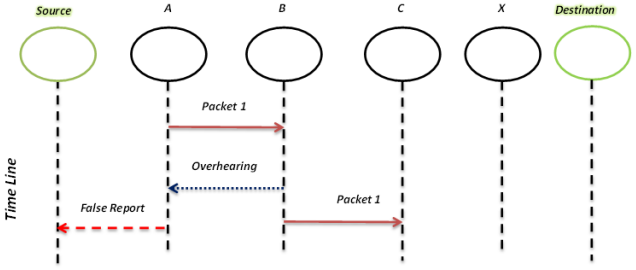

Figure 6. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

2. 2. Two Acknowledgment IDS (TWO-ACK)

It is another important IDS TWO-ACK for discovering malicious nodes in MANETs [22]. The main aim of this ID to resolve the receiver collision and limited transmission power problems of Watchdog, TWO-ACK 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 along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWO-ACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

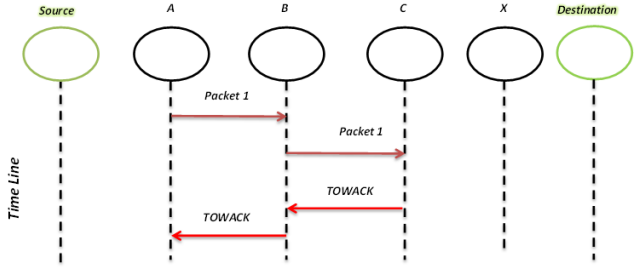

Figure 7. TWO-ACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The TWOACK IDS effectively processes the receiver collision and limited transmission power problems indicated by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

2.3. Adaptive Acknowledgment IDS (AACK)

It is same as TWO-ACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an ID called TACK (identical to TWO-ACK) and an end-to-end acknowledgment IDS called Acknowledge (ACK). Compared to TWO-ACK IDS, AACK IDS reduced network overhead. The end-to-end ACK IDS is shown in Fig 8.

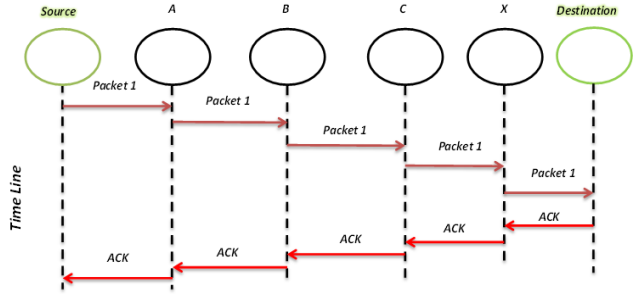

Figure 8. End-to-End ACK IDS for MANETs ACK scheme: The destination node is required to send acknowledgment packets to the source node.

The source node sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node along the reverse order of the same path. Within a predefined time slot, if the source node receives this ACK packet, then the packet transmission from node Source to node Destination is successful.

But both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and fake ACK packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWO-ACK and AACK. The functions of such detection schemes all largely depend on the ACK packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

2.4. Enhanced Adaptive Acknowledgment IDS (EAACK)

EAACK is based on both DSA and RSA algorithm. The three main parts of the EAACK scheme are ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). EAACK is an acknowledgement based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets. Before the acknowledgement packets sent out EAACK requires the whole acknowledgement packets are digitally signed and verified by its receiver until they are accepted.

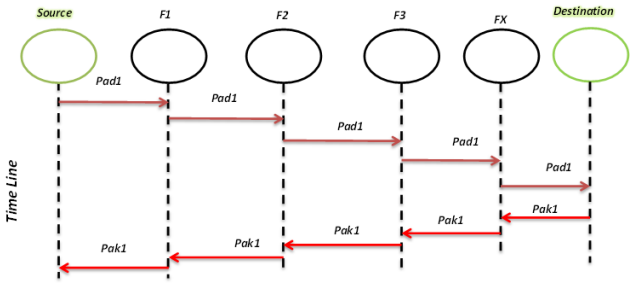

Figure 9. System control flow: This figure shows the system flow of how the EAACK scheme works.

3. Proposed System (HCEAACK) Hybrid Cryptography Enhanced Adaptive Acknowledgment

Our Proposed model (HCEAACK) is consisted of four major modules:

3.1. Basic Routing Module

If the source has no route to the destination, then source initiates the route discovery in an on-demand fashion . After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

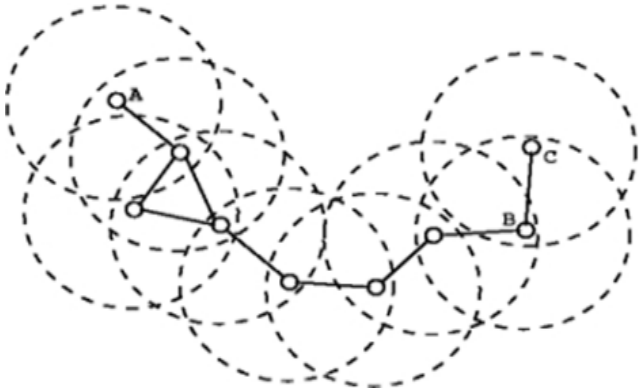

Figure 10. Basic Routing[18]

3.2. Secrete Acknowledgement Module

Secrete Acknowledgement ACK is principally end-to-end acknowledgement scheme. Intend to reduce network overhead when no network misbehavior is detected. In the Secrete ACK mode, the Source node sends the ACK data packet to the destination node. After that, the intermediate nodes between the source and destination are cooperative and after Destination node successfully receives Packet it requires to send the Secrete ACK packet back to the Source node (after applying a hybrid cryptography technique) with same route but in reverse order. If in a particular time the Source node receives the Secrete ACK packet the data transmission is successful. Otherwise, Source node will change to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes.

3.3. Secure Acknowledgement (S-ACK) Module

In the S-ACK scheme to detect the misbehaving nodes every three successive nodes work in a group. In the three successive nodes the Secrete acknowledgment packet is sent by the third node to the first node. The S-ACK scheme is able to detect the misbehaving nodes in the presence of receiver collision and low transmission power. If Secrete acknowledgement not received means it will report those nodes as misbehaving nodes to source node. But in this process there is a chance of false reports, to avoid this we are implementing Misbehavior Report Authentication (MRA) Module.

3.4 MRA Misbehavior Report Authentication Module

Because of false report information the IDS reports normal nodes as malicious nodes. To overcome this problem, the MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. For this the source node seeks its local knowledge base and identifies the other route to the destination node. If there is no route to destination by using

the DSR routing request to find the alternate route. When the MRA packet is received by the destination node, it compares with using the local knowledge base whether the reported packet was received or not. If already received it make a decision, it is a false misbehavior report.

4. Implementation of Proposed Model

In our proposed model, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets described in this model are required to encrypted and digitally signed by its sender node before they are sent out and verified by its receiver node until they are accepted, for this purpose we use hybrid cryptography Technique.

4.1 Hybrid Cryptography Technique

This hybrid cryptography Technique uses two algorithm, Advanced Encryption Standard (AES) algorithm and RSA algorithm which cooperated to give more security for Secrete acknowledgment packets in our proposed model**.** We assumed that both a public key, private key and Secret key are generated for each node and they were all distributed in advance.

Our hybrid cryptography Technique for the proposed model consists of two processes:

- ❖ Formation process for secrete acknowledgment packet at Destination Node.
- ❖ Verification Process for secrete acknowledgment packet at Source node.

After destination node received the data packet from the source node it must send back Acknowledgment packet. Here our proposed hybrid cryptography Technique starts with formation process of Secrete Acknowledgement at Destination Node. The secrete Acknowledgment packet produced by encryption the acknowledgment packet using AES algorithm with secret key and then digital sign the encrypted Acknowledgment packet using RSA algorithm(using private key).

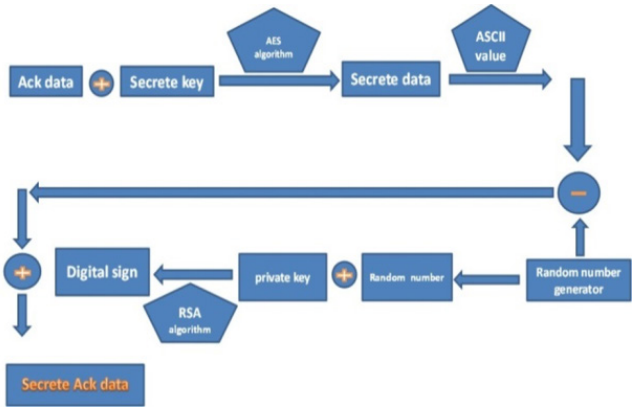

Figure 11. Formation of Secrete Acknowledgement packet at Destination Node.

Figure 11 shows the formation of secrete Acknowledgement packet by the destination node. Secrete key used to make more security for acknowledgement packet and encrypted ACK data by AES algorithm. Then RSA algorithm has been used to produced digital sign for the secrete data and then get the secrete acknowledgement packet ACK that send to source node.

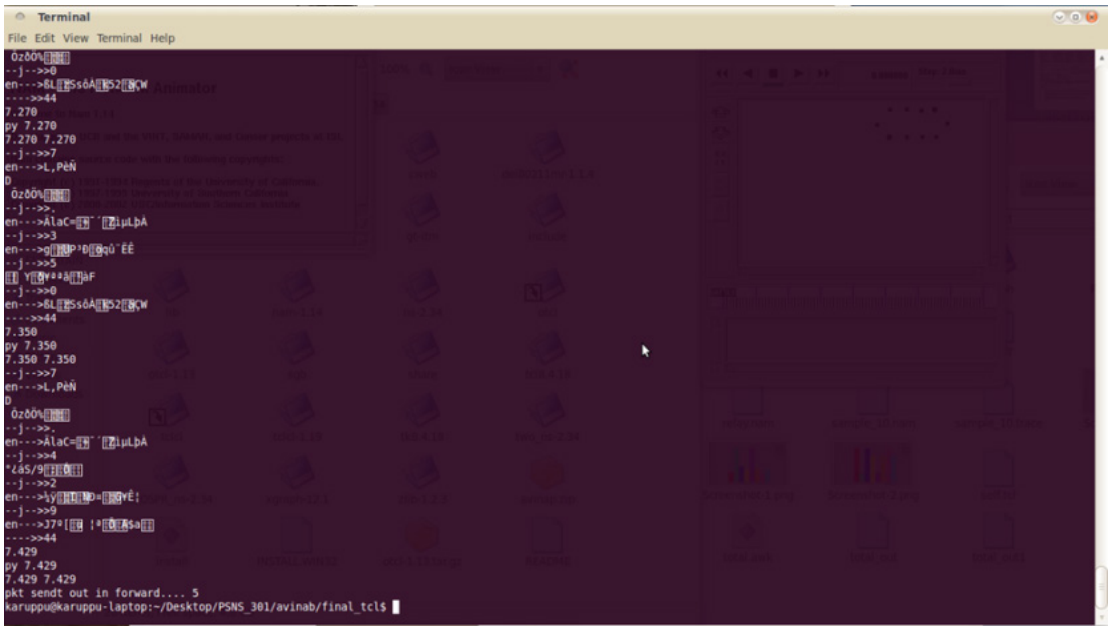

Figure 12. Encrypted Acknowledgment packet by AES algorithm.

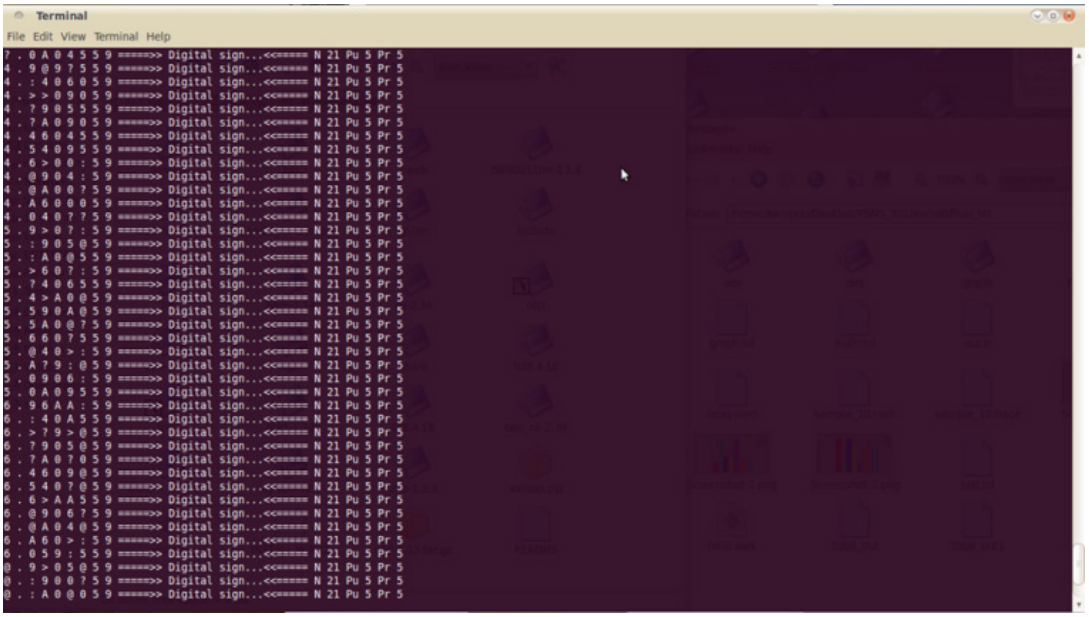

Figure 13. Digital Sign of encrypt Acknowledgment packet by RSA algorithm.

The second process of our proposed hybrid cryptography Technique for Verification Process for secrete acknowledgment packet begin after source node receive the secrete acknowledgment packet from the destination node, it first verify digital sign using RSA algorithm(with public key), then it use AES algorithm and depending on secrete key to verify acknowledgment packet from the destination node.

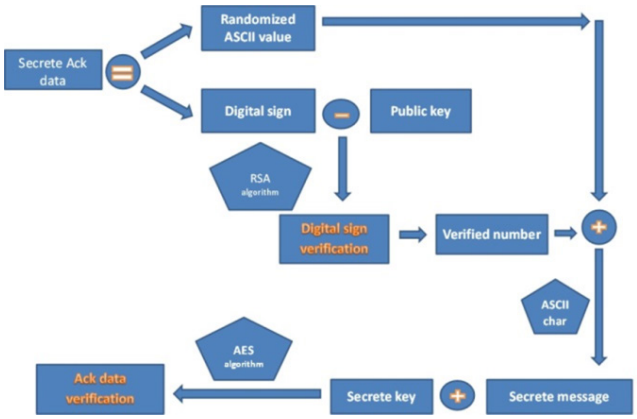

Figure 14. Verification Process at Source node.

Figure 14 show the Verification process at source node after receive the secrete ACK .First the source node verify digital sign for the secrete ACK using RSA algorithm, then it use AES algorithm and depending on secrete key to verify ACK from the destination node.

4.2. Algorithm of Proposed Model

1) If node has data to transfer to destination node

a. Check the routing table

i. If route found

1. Send the data
2. Start Counting data
3. At beginning of data count set the timer to check the counting

ii. If route not found

1. Generate the Request (Req) as normal on demand routing protocol
2. Update the request with own public key
3. Broadcast to all neighbor to find destination

2) I If Request (Req) received

a. Checks Req is new

i. If not

1. Ignore

ii. If yes

1. Updates the reveres route
2. Updates the key information
3. Checks node is the destination
   a. If yes
      i. Generate the Replay (Rep) with own public key
   b. If not
      i. Forward the packet further to all

3) If Replay (Rep) received

a. Updates reverse route

b. Updates the key information

c. Checks node has data to send to source of reply

i. If yes

1. Go to main step 1

d. Checks the route to rep destination

i. If found

1. Forward

ii. Else
1. Ignore

4) If data received

a. Checks I'm the destination
i. If yes
1. Generate the ACK
a. Set current time as ACK time *Ta*
b. Checks the pair-wise key between source and destination
i. If found set key as $K_{S_{s-d}}$
c. Split *Ta* into separate character $\cup T_{sA}$
d. Create empty list for encrypted data *El*
e. For-each char $Pt \in T_{sA}$
i. Encrypt by AES algorithm
1. Pt => Ct
2. Convert to ASCII value Cta
3. Generate random number(rand)
4. New value Nv = Cta-rand
5. (Cta & Nv& rand) ∪ El
ii. Make digital sign
1. Checks for own private key
2. For each value of El
a) Extract *Nv*
b) Encrypt by RSA private key
i. Nv ==> CNv
ii. CNv ∪dgital_sgn_lst
3. Send the secrete ACK with
a. Digital sign
b. Rand number
c. Generation time

5) If digital sign received in source

a. Node checks the public key info for ACK generator
i. If found
1. decrypt by *Pu ===> Ptrsa*
2. Checks for secrete pair key
a. If found
i. Decrypt *Ptrsa* by *K_(S_(s-d))* ==>Pt
3. Pt U plain text list
b. Compare with original form of digital sign with plain text list data
i. If matching
1. Forward further data through same path
ii. If not matching
1. Switch to secure ACK mode

```
Initiate S-ACK
If (Received data == S ack) {
Misbehavior report (a);
If (Misbehavior report (a) ==0)
{
Send D ack;
} else {
Initiate MRA mode;
}
If (Received data == MRA) {
Find another path to Destination;
If (Destination node doesn't have packet) {
Trust the report
} else {
Mark reporter as malicious;
}
Create a list H (i); # storing information about malicious nodes;
}
```

5. Simulation Configuration and System Run

Our simulation is conducted within the Network Simulator NS2.34 environment on a platform Ubuntu 10.04. The system is running on a laptop with Core i5 3210M CPU and 4-GB RAM. In NS2.34, the configuration specifies 10 nodes in a flat space with a size of 670 × 670 m. with single source and destination with possible of two routes. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 10ms. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. The packets are routed using Ad hoc On-demand distance vector routing protocol and the acknowledgments Packets are authenticated using RSA and AES algorithm.

We test our proposed model with other intrusion detection system in many scenarios which it:

1- BAODV: Basic Ad-hoc On Demand Vector scenario.
2- BAODV_meli: Basic Ad-hoc On Demand Vector with malicious node scenario.
3- TWO-ACK: two Acknowledgment ID scenario.
4- AACK_meli : Adaptive Acknowledgment ID with malicious node scenario.
5- AACK_Fmeli: Adaptive Acknowledgment ID with Fake Acknowledgment malicious node scenario.
6- EAACK_meli: Enhance Adaptive acknowledgment ID with malicious node scenario.
7- EAACK_Fmeli: Enhance Adaptive Acknowledgment ID with Fake Acknowledgment malicious node scenario.
8- HCEACK: Hybrid Cryptography Enhanced Adaptive Acknowledgment ID scenario.

And for each scenario we estimated the values of three performance metrics Packet delivery factor (PDF), Routing Overhead (OH) and Average end-to-end delay (D) to

evaluate the performance of IDS for existing and proposed technique.

BAODV: Basic Ad-hoc On Demand Vector scenario Data Transmission from Source to Destination without any Security Data Transmission without any Acknowledgment sharing. So if there is any malicious node found in the path means node can't detect the malicious node information.

(BAODV_meli) Basic Ad-hoc On Demand Vector with malicious node scenario when malicious node appears the Packet delivery factor PDF drop and the Delay time increase in network.

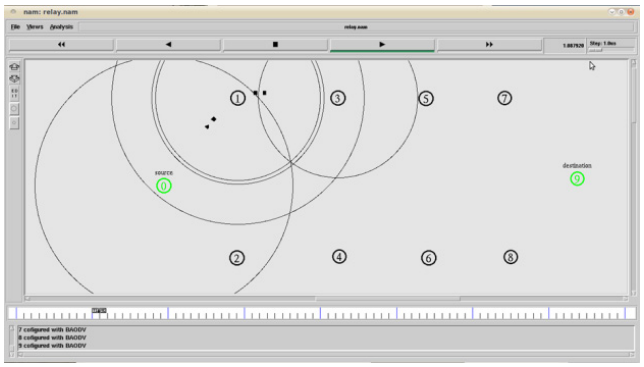

Figure 15. BAODV: Basic Ad-hoc On Demand Vector scenario.

In TWO-ACK scheme while transferring the data each node need to generate the Acknowledgment ACK after receiving the data and that should be forwarded to previous node. And at the same time each node has to forward the Acknowledgment ACK of next node to previous node. By this method we can find the intermediate malicious node.

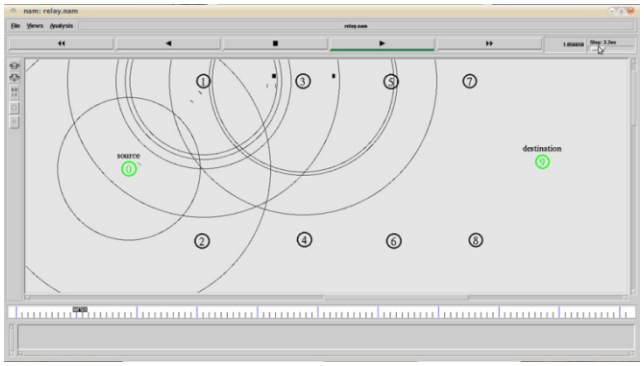

Figure 16. TWO-ACK: two Acknowledgment ID scenario.

But this method increases the network load while sharing the number of acknowledgement.

By using AACK method we can provide same security as well as reduced overhead. In this scheme before attack end-to-end Acknowledgment ACK used to reduce the overhead and while attack the source node will switching to TWO - ACK model node to find the malicious node.

In (EAACK_meli) Enhance Adaptive acknowledgment ID with malicious node scenario (as we see in figure 17). Malicious Node Collects the Data but there is No ACK to Source the malicious node can't generate the ACK so by that source can find attack, and source will switch to secure ACK (S-ACK) mode to find the malicious node.

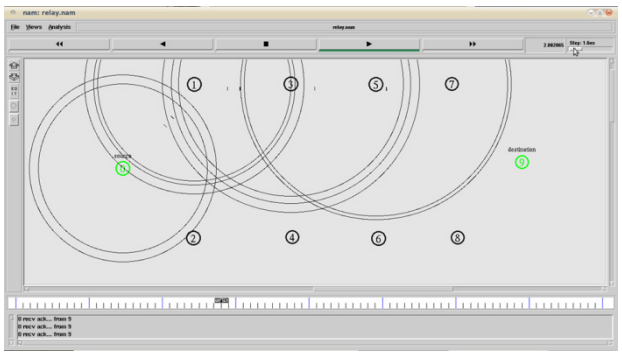

Figure 17. end-to-end Acknowledgment ACK (EAACK model)

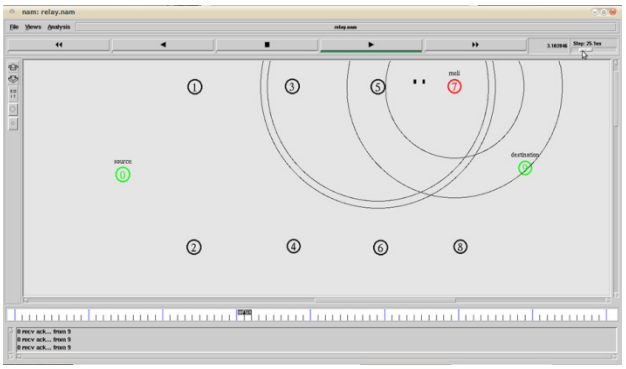

Figure 18. Adaptive Acknowledgment ID with malicious node scenario.

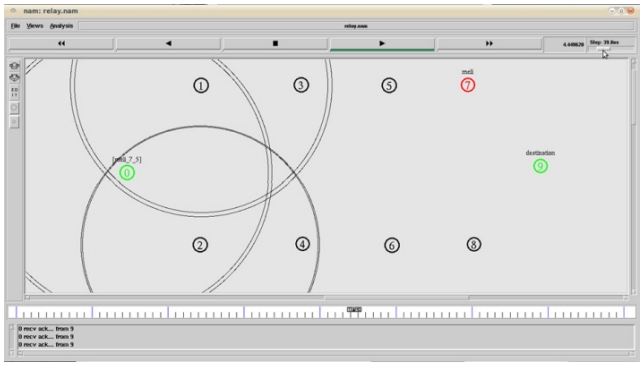

Figure 19. Checks the New Route after Finding the Malicious.

AACK method considered the malicious can't send the ACK. But attacker may chances to send the fake ACK (AACK_Fmeli: Adaptive Acknowledgment ID with Fake Acknowledgment malicious node scenario). In this case AACK can't detect the attack.

To improve this method EAACK method has been implemented. By this method we can find normal malicious. EAACK requires all acknowledgment packets to be digitally signed using RSA algorithm before they are sent out and verified until they are accepted. In RSA algorithm, public key and Private Key used to share the secrete. The keys are denoted as public key (e, N) and Private Key (d, N) to generate keys we have to use two prime numbers by key generation. To make encryption decryption the nodes should

share the public key (e, N) to all other node. By using public key (e, N) value, the hacker can find private key (d, N) by using RSA hacking like reverse formulation.

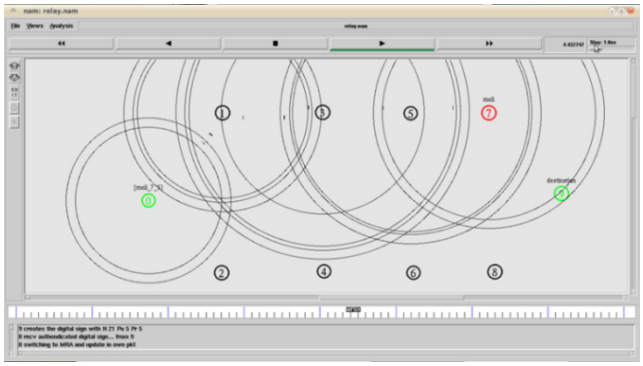

Figure 20. Enhance Adaptive Acknowledgment ID with Fake Acknowledgment malicious node scenario.

To solve the prblem of forged acknowledgment attacks we run our proposed model Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK) ID scenario with hybrid cryptography Techniqe. Including Hybrid Cryptography in HCEAACK to prevent the attackers from initiating forged acknowledgment attacks(like RSA hacking). In the HCEAACK all acknowledgement packets are encrypted and digitally signed before they sent out and verified until they are accepted.

6. Performance Evalution of Proposed Model

To provide a better insight on our simulation results, detailed simulation data recorded are presented in result Table.

Table 1. Result table

Model	Packet delivery factor PDF (%)	overhead OH	Delay(ms)
BAODV	100	16	108
BAODV_meli	28.40	16	367
Two_ACK	99.122	854	168
AACK_meli	79.54	400	144
AACK_Fmeli	28.40	393	367
EAACK_meli	79.54	400	144
EAACK_Fmeli	98.86	488	116
HCEAACK	79	400	144

Result in table 1 show that In BAODV model there is no ACK sharing so overhead is very less, but when malicious node appear (BAODV_meli) model the Packet delivery factor PDF drop and the Delay time increase in network, in Two_ACK mode there are numbers of ACK shared between each node so network overhead and delay is increased. When considered normal attack with AACK method, in this case AACK method can find the malicious and it should change the path so packet delivery is less compare than the BAODV, but at the same time AACK can't find fake ACK so it reduces the further packet delivery factor (PDF) in fake ACK scenario (AACK_Fmeli).EAACK and HCEAACK can provide good performance in fake ACK scenario and normal malicious scenario, and our proposed model HCEAACK give best packet delivery factor (pdf) on same value of network overhead with best protection level for acknowlegment packet from attacks like RSA hacking that apper in EAACK model .

In order to measure and compare the performances of our proposed model, we continue to adopt the following three performance metrics to evaluate the performance of IDS for existing and proposed technique which are defined as follows:

1. Packet delivery factor (PDF)

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

$$\text{PDF} = \frac{\sum \text{Received packets at destination}}{\sum \text{Sent packets by sources}} \quad (1)$$

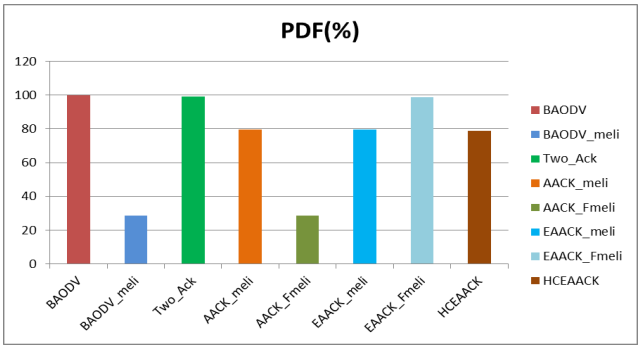

Figure 21. comparison of Packet delivery factor pdf

2. Routing Overhead (OH) 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.

$$\text{OH} = \frac{\sum \text{Routing transmissions}}{\sum \text{Data transmissions} + \sum \text{Routing transmissions}} \quad (2)$$

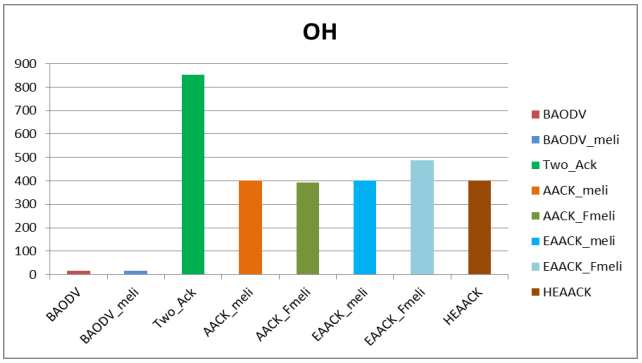

Figure 22. comparison of overhead

3. Average end-to-end delay (D) The average end-to-end delay for all successfully received packets at the destination.

It is calculated for each data packet subtracting the sending time of the packet from the received time at final destination.

$$D = \frac{\sum_1^N (T_{Rceived} - T_{Sent})}{N} \quad (3)$$

Where N is number of successfully received packets.

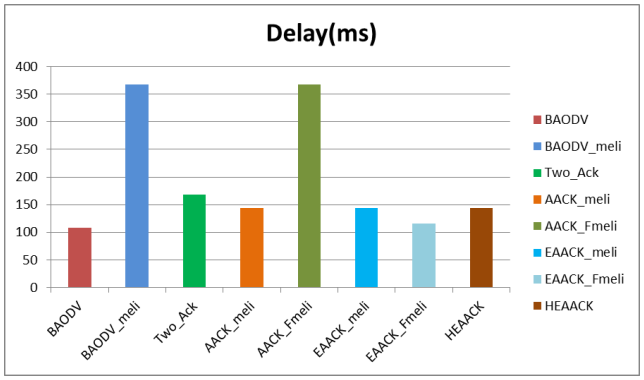

Figure 23. comparison of delay

7. Conclusions and Future Work

To provide security in the mobile Ad-hoc networks we implementing a new intrusion-detection system named Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK). Including Hybrid Cryptography in HCEAACK to prevent the attackers from initiating forged acknowledgment attacks like RSA hacking. In the HCEAACK all acknowledgement packets are encrypted and digitally signed before they sent out and verified until they are accepted. The proposed Model completely overcomes the weaknesses like false misbehavior, limited transmission power, and receiver collision. All acknowledgment packets in the proposed Model are authentic and untainted. The proposed model can significantly improve the Packet Delivery Factor (PDF).

To increases the merits of our research work; we plan to investigate the following issues in our future research:

1) Examine the possibilities of adopting a key exchange mechanism that does not require any Trusted Third Party (TTP) for key management to eliminate the requirement of pre distributed keys.

2) Testing the performance of our proposed model (HCEAACK) in real network environment instead of software simulation.

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, ―Which wireless technology for industrial wireless sensor networks? The development of OCARI technology, ‖ IEEE Trans. Ind. Electron., vol. 56, no.10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, \Mobile Ad hoc Network Security,in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659.666.

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

[4] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[5] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[6] R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey, ‖ in Proc. 2nd Int.Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[7] T. Anantvalee and J. Wu, ―A Survey on Intrusion Detection in Mobile Ad Hoc Networks, ‖ in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[8] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ.Press, Aug. 2007.

[9] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, ―Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks, ‖ IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766,Jul. 2008.

[10] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,pp. 2759–2766, Jul. 2008.

[11] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[12] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[13] 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.

[14] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf.Pervasive Comput. Commun., 2005, pp. 191–199.

[15] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819,Mar. 2010.

[16] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[17] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric

micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[18] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[19] E .Shakshuki and Nan Kang "EAACK - A Secure Intrusion-Detection System for MANETs," IEEE TRANSACTIONS ON INDUSTRIAL ELEC., VOL. 60, NO. 3, MARCH 2013.

[20] 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.

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

[22] "A study of different types of attacks on multicast in mobile ad hoc networks" Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier AdHoc Networks(2008) 32-46.