ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Design of EEACK Protocol for Partial Dropping in Watchdog Security Scheme

S. Sri Gowthem[1], K.P. Kaliyamurthie[2]

[1]Assistant Professor, Department of CSE, Bharath University, Chennai, Tamil Nadu, India

[2]Professor & Head, Department of CSE, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly are indirectly. MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure , thus all nodes are free to move randomly. Open medium and remote distribution of MANET make it vulnerable to various types of attacks. Due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. MANET is a open medium so it have lot of security issues in that so to overcome all this defects there are several protocols that are implemented to address this security issues are watchdog and AACK(Adaptive acknowledgement protocols). This two protocols had overcome some of the problems like receiver collisions and limited transmission power but this protocols still fails to address false misbehavior report. In this work a new scheme called EEACK (EnhancedAdaptiveAcknowledgement protocol) consists of three major parts namely ACK, secure ACK(s-ACK) and misbehavior report authentication(MRA). By using all this various steps here overcome the existing problem of watchdog scheme like false misbehavior report and partial dropping.

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days . 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. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry, However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic.

II. BACKGROUND

A. IDS in MANETs

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog TWOACK and Adaptive ACKnowledgment (AACK)

***1.Watchdog**:*

Marti *et al.* [17] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node 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, 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. Many following research studies and implementations have
proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field.
Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Nevertheless, as pointed out by Marti *et al.* the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping. We discuss these weaknesses with further detail.

2) TWOACK:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems 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 along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).The working process of TWOACK is Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed 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. However, many research studies are working in energy harvesting to deal with this problem.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

3) AACK:

Based on TWOACK, Sheltami *et al.* proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered 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 significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK.

In the ACK scheme, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, 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 forged acknowledgment packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

B. Digital Signature

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical
techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The development of cryptography technique has a long and fascinating history. The pursuit of secure communication has been conducted by human being since 4000 years ago in Egypt, according to Kahn's bookin 1963. Such development dramatically accelerated since
the World War II, which some believe is largely due to the globalization process.
The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and nonrepudiation . Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature. Digital signature schemes can be mainly divided into the following two categories.
1) *Digital signature with appendix*: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA)
2) *Digital signature with message recovery*: This type of scheme does not require any other information besides the signature itself in the verification process. Examples
include RSA.

III. PROBLEM DEFINITION

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses in detail.

IV. SCHEME DESCRIPTION

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR, there is 6 b reserved in the DSR header. In EAACK, we use

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

2 b of the 6 b to flag different types of packets. Details are listed presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, 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.Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

A. ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 8, in ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the
route.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [16]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. in S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *Psad*1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives *Psad*1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 forwards *Psak*1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we
circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowlknowledge base and compares if the reported packet was received. If itis already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.[1] With regard to this urgent concern, we incorporated digital signature in our proposed

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

V. PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.[2]

A. Simulation Methodologies

To better investigate the performance of EAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: In this scenario, we simulated a basic packetdropping
attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog,
namely, receiver collision and limited transmission power.

Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious
nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is used to test the IDSs' performances when the attackers are smart enough to forge acknowledgment
packets and claiming positive result while, in fact, it is negative.[3] As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting

C. Performance Evaluation

To provide readers with a better insight on our simulation Results

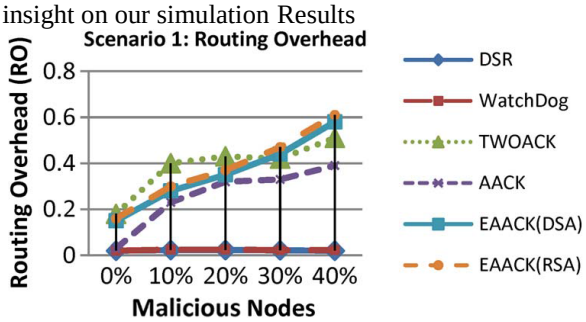

Fig. 1. Simulation results for scenario 1—RO.

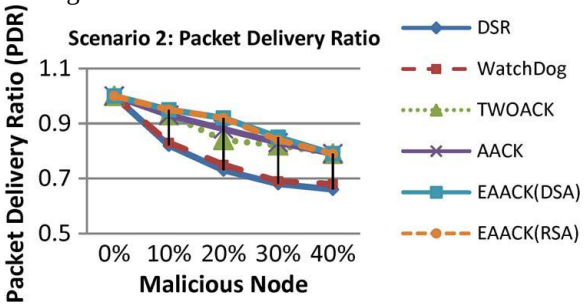

Fig. 2 Simulation results for scenario 2—PDR.

when there are 20% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

including TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power.[4] However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's
performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold. The simulation results of RO in scenario 1 are shown in Fig. 11. We observe that DSR and Watchdog scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors.[5] For the rest of the IDSs, AACK has the lowest overhead. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases. We conclude that this happens as a result of the introduction of our hybrid scheme.

2) Simulation Results—Scenario 2:

In the second scenario,we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible.[6] This scenario setting is designed to test the IDS's performance under the false misbehavior report the achieved simulation results based on PDR. When malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report.In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more

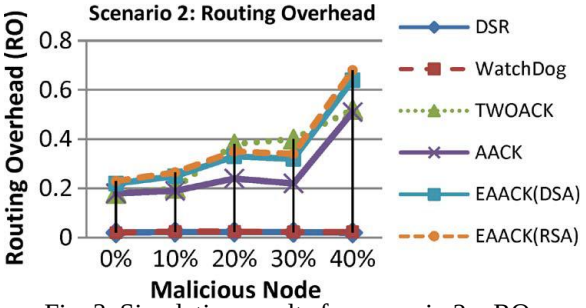

Fig. 3. Simulation results for scenario 2—RO.

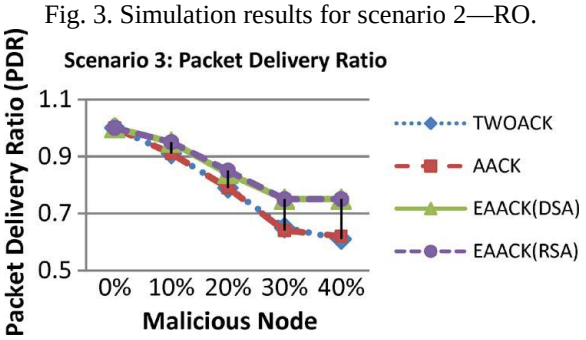

Fig.4. Simulation results for scenario 3—PDR.

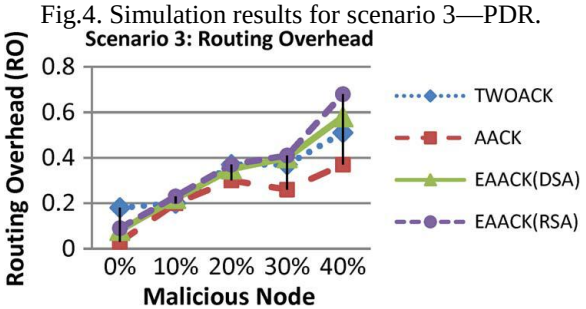

Fig.5. Simulation results for scenario 3—RO.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

malicious nodes require a lot more acknowledgment packets and digital signatures.

3) Simulation Results—Scenario 3:

In scenario 3, we providethe malicious nodes the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary.[7] This is a common method for attackers to degrade network performance while still maintaining its reputation. The PDR performance comparison in scenario 3 is shown In We can observe that our proposed scheme EAACK outperforms TWOACK and AACK in all test scenarios. We believe that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets. shows the achieved RO performance results for each IDS in scenario 3. Regardless of different digital signature schemes adopted in EAACK, it produces more network overhead than AACK and TWOACK when malicious nodes are more than 10%. We conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes.[8]

4) DSA and RSA:

In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does.[9] This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.[10]

VI. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

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

1) possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys;
3) testing the performance of EAACK 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 technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
[2] Vijayaragavan S.P., Karthik B., Kiran T.V.U., Sundar Raj M., "Robotic surveillance for patient care in hospitals", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp. 1820-1824
[3] 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

[4] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., Sundar Raj, M."Analysis of chaotic DC-DC converter using wavelet transform", Middle - East Journal of Scientific Research, ISSN : B27, 16(12) (2013) pp.1813-1819.
[5] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc net works: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012, pp. 535–541.
[6] Vijayaraghavan K., Nalini S.P.K., Prakash N.U., Madhankumar D.,"Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum", Materials Letters, ISSN : 0167-577X, 75() (2012) pp. 33-35.
[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] Vijayaraghavan, K., Nalini, S.P.K., Prakash, N.U., Madhankumar, D., "One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum", Colloids and Surfaces B: Biointerfaces, ISSN : 0927-7765, 94() (2012) pp. 114-117.
[9] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[10] Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", Biomedicine and Preventive Nutrition, ISSN : 2210-5239, 2(4) (2012) pp.252-259.
[11] Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014
[12] Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014
[13] Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014
[14] KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.
[15] .Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013