An Acknowledgement based Intrusion Detection System using ECDSA for Detecting Malicious Node in MANET

T.Elaya Perumal
ME / CSE
King College of Technology

P.Kuppusamy
ASP / CSE
King College of Technology

S.Chandra
AP / CSE
Selvam College of Arts & Science

ABSTRACT

Mobile Ad hoc network is a group of wireless mobile nodes generating a network not by using any existing infrastructure. MANET is a collection of mobile nodes equipped with a wireless-transmitter and receiver that in contact with each other via bi-directional wireless links either directly or indirectly. An encroachment detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the acceptation of MRA scheme, EAACK is capable of finding malicious nodes contempt the existence of the false misbehavior report and equate it against other popular mechanisms in different scenario through simulation. The results will exhibit positive performances against thefalse misbehavior report. EAACK demonstrates higher leering behavior detection rates in certain circumstances while does not greatly affect the network performances.Malicious attackers to falsely report innocent nodes as malicious can produce the false misbehavior report. EAACK is an acknowledgment-based encroachment detection system.This attack can be deadly to the entire network when the attackers break down sufficient nodes and thus cause a network division.The introduction of digital signature (DSA) is to prevent the attacker from counterfeitacknowledgment packets.

Keywords

Enhanced AdaptiveAcknowledgement MANET, Elliptical curve digital signature

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is an aggregation 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. One of the important advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility [17]. MANET is capable of making a self-configuring and self-maintaining network not by the help of a centralized infrastructure, which is often impracticable in critical mission applications like military conflict or emergency recovery. Minimum configuration and speedy deployment make MANET ready to be used in emergency context where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced catastrophe, military battles, and medical emergency situations. Regrettably, the open medium and remote distribution of MANET make it defendable to various types of attacks.Most routing protocols in MANETs considering that every node in the network act as cooperatively with other nodes and presumably not deliberately harmful, attackers can easily compromiseMANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS)specially designed for MANETs.

1.1Benefits

Having discussed the general issues in MANETs, thebehind their popularity and their benefits will nowbe discussed.

(a) ***Low cost of deployment***: As the name suggests, adhoc networks can be deployed on the fly, thus demandingno expensive infrastructure such as copperwires, data cables, etc.

(b) ***Fast deployment***: When conceded to WLANs, adhoc networks are very convenient purpose and easy to deployrequiring less manual intervention sincethere are no cables involved.

(c) ***Dynamic Configuration****:* Ad hoc network configurationcan change dynamically with time. For themany scenarios such as data sharing in classrooms, etc., this is a useful feature. When comparedto configuration of LANs, it is very easyto change the network topology.

2. RELATED WORK:

Each node in MANETs assumesthat other nodes always work together with each otherto relay data. This premise leaves the attackerswith the opportunities to achieve significant impact onthe network with just one or two compromised nodes. To eliminate the potential damages caused by compromisedaddress this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs.If MANET can detect the attackers as soon asthey enter the network, this paper will be able to completelynodes at first time. IDSs usually act as the secondlayer in MANETs, and it is a great complement to existingproactive approaches and presented a very thoroughsurvey on contemporary IDSs in MANETs [3]. In this section, theymainly describe three existing approaches,namely, Watchdog [10], TWOACK [12] and AACK [15]. Thewatchdog scheme [10] is consisted of two parts, namelyWatchdog and Path rates. Watchdog serves as anintrusion detection system for MANETs. It is responsiblefor detecting malicious nodes misbehavior in thenetwork. Watchdog detects malicious misbehavior bypromiscuously listens to its next hop's transmission. IfWatchdog node overhears that its next node fails to forwardthe packet within a certain period of time, it increasesits failure counter.Whenever a node's not success counter exceeds a predefinedthreshold, the Watchdog node reports it as misbehaving.In this case, the Path rates get together with therouting protocols to avoid the reported nodes in futuretransmission. ManyMANET IDSs are either based on or developed as animprovement to the Watchdog scheme.

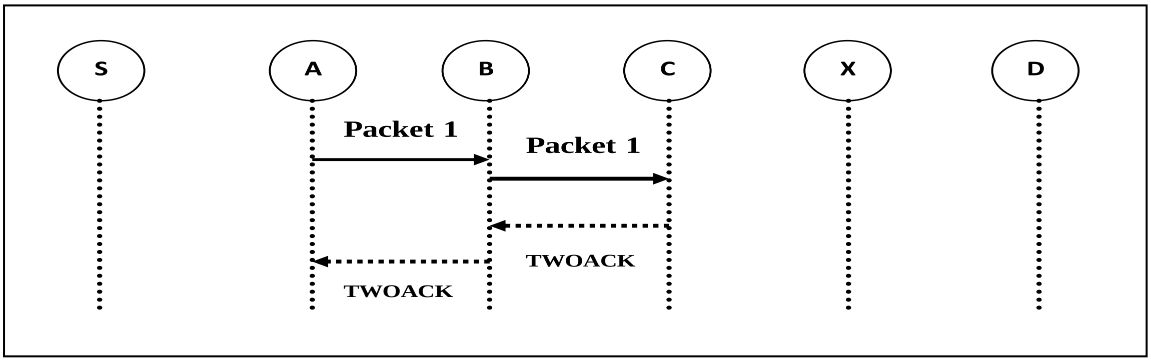

Fig.1. Two way Acknowledgement

Watchdogscheme fails to detect deliberately harmful misbehaviourwith the presence ofambiguous collisions, receiver collision,limited transmission power,false misbehaviour report,collusionand partial dropping.TWOACK [18] is neither an agreeable nor a Watchdogbased scheme. Aiming to resolve the receivercollision and limited transmission power problems ofWatchdog, TWOACK finding misbehaving links by acknowledgingevery data packets transmitted over each one after the otherthree nodes along the path from the sourceto the destination.

Upon retrieval of a packet, each nodealong the route is needed to send back an acknowledgementpacket to the node that is two hops away fromit down the route.AACK is based on TWOACK Acknowledgement (AACK) similar to TWOACK, AACK[15] is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. EAACK is intentional to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision [19].The Introduction of digital signature is 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).

ACK is basically an end-to-end acknowledgment scheme. In ACK mode, node S first sends out an ACK data packet Pad1 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 Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined timeperiod, if node S receives Pak1, 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.

The S-ACK scheme is a latest version of the TWOACK scheme.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 current existence of receiver collision or limited transmission power.Unlike the TWOACK scheme, where the Source node immediately trusts the misbehaviour 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 the proposed scheme.

Misbehavior report assay-markscheme [19] is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.EAACK is an acknowledgment-based Intrusion Detection system. 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.EAACK [19] requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted [19]. They have presented the digital signature algorithm is to sign the acknowledgement packet, it normally involve more network overhead and energy consumption.

3. METHODOLOGY

Enhanced adaptive acknowledgement (EAACK) is an acknowledgement based intrusion detection system; in order to ensure all acknowledgement packets is authentic. They use digital signature algorithm (DSA) to sign the acknowledgement packets, digital signature algorithm (DSA) involves more routing overhead and energy consumption, Adopting hybrid cryptography techniques.To further reduce the network overhead caused by digitalSignaturewithout compromising its security. This paperproposesElliptic curve Digital signature algorithm instead of Digital Signature Algorithm to ensure that all acknowledgment packets in EAACK are authentic and untainted.ECDSA stands for “Elliptic Curve Digital Signature Algorithm”, it’s used to create a digital signature of data (a file for example) in order to allow you to verify its authenticity without compromising its security. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses elliptical curve cryptography.

Elliptical curve cryptography is consider on an equation of the form: ***y^2 = (x^3 + a * x + b) mod p.***To sign amessage, the curve parameters **(CURVE, G, n)** must be agreed upon. In addition to the field and equation of the curve, Need G,a base point of prime order on the curve; **n** is the multiplicative order of the point **G**.A private key integer dA, randomly selected in the interval (1,n-1); and a public key curve point **QA=dA * G**.

Use * to denote Elliptical curve point multiplication by scalar. To sign a message m**,** follows these steps.

1. Compute**e=HASH (m)**, where HASH is a cryptographic hash function, such as **SHA-1**.

2. Let z be the **Ln** leftmost bits of e, where **Ln** is the bit length of the group order **n**.

3. Select a random integer **k** from **(1,n-1)**.

4. Compute the curve point **(x1, y1) =k*G.**

5. Compute **r = x1 mod n**. If **r=0,** back to step 3.

6. Compute**s=** k^{-1}**(z + rdA).**If **s=0**, back to step 3.

7. The signature is the pair **(r, s)**.

To Signature verification

To authenticate signature, must have a copy of her public key curve point **QA**. Verify that r and s are integers in **(1, n-1).** If not, the signature is invalid.

1.Compute**e=HASH (m)**, where HASH is the same function used in the signature generation.

2. Let **z** be the **Ln** leftmost bits of **e**.

3. Compute **w =**s^{-1} **mod n.**

4.Compute **u1=zw mod n** and **u2= rw mod n.**

5.Compute the curve point **(x1, y1)=u1 * G +u2 *QA**. .

6.The signature is valid if **r= x1 (mod n)**, invalid otherwise.

Normally data transmission in MANETs consumes the most battery power. Hence Elliptic curve Digital signature algorithm requires less computational power than Digital Signature Algorithm. Proposed scheme always produces slightly less network overhead than DSA does.Shorter keys are as strong as long key for DSA, Low on CPU consumption and memory usage.

4. PERFORMANCE EVALUATION

In this paper concentrate on describing the simulation environment and the system of methods followed in a particular discipline as well as comparingperformances through simulation result comparison with EAACK schemes.

4.1 Simulation setup

The simulation is carry on within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10[19]. The system is running on a laptop with Core 2 Duo T7250 CPU and 2-GB RAM. In order to better compare this work simulation results with other research works, this paper adopted the default scenario settings in NS2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the defaultconfiguration specifies 50 nodes in a flat space with a size of 700m × 700 m.

The maximum hops allowed in this configuration setting are four. 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 20 m/s and a pause time of 1000s. User Datagram Protocol traffic with constant bit rate is enforced with a packet size of 512 B. In order to measure and compare the public presentation of theproposed scheme, this paper continues to adopt the following four performance metrics [8].

4.2 Metrics

4.2.1*Packet delivery ratio*

PDR defines the ratio of the number of packets standard by the destination node to the Number of packets sent by the source node.

4.2.2*Routing overhead*

RO defines the ratio of the amount of routing-related transmissions.[Route Request(RREQ), Route Reply (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

4.2.3*Total energy consumption*

Total energy ingestion metric in EAACK illustrates the total amount of energy consumed by each node in the network.

4.2.4*Inter arrival packet time*

Interarrival packet time metric in EAACK is the time taken by the packet to reach the finishing node from the source node.During the computing, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ messagemore than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocol like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its destination node, the destination node initiates an RREP message and sends thismessage back to the source node by reversing the route in the RREQ message.

About the digital signature schemes, this paper adopted an open source library named Botan [4]. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA [17] and RSA schemes, this paper generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. This paper assumed that both a public key and a private key are generated for each node and they were all distributed in advance. The typical sizes of public and private-key files are 654 and 509 B with a 1024-b DSA key, respectively. On the other hand, the sizes of public and private-key files for 1024-b RSA are 272 and 916 B, respectively. The signature file sizes for DSA [17] and RSA [14] are 89 and 131 B, respectively. In terms of computational complexity and memory expenditure, this paper did research on popular mobile sensors. According to this research work, one of the most popular sensor nodes in the market is Tmote Sky [19]. This type of sensor is equipped with a TI MSP430F1611 8-MHz CPU and 1070 KB of memory space. Believe that this is enough for handling the simulation settings in terms of both computational power and memory space.

5. RESULTS AND DISCUSSION

In order to measure and compare the performance of proposed scheme, this paper continues to espouse the following four performance metrics [9].

5.1 Routing overhead

Routing Overhead defines the ratio of the amount of routing-related transmissions. Routing overhead rises rapidly with the increase of malicious node. When malicious node is 20%, the proposed scheme performs better than EAACK (DSA). It is due to the Elliptical curve DSA. In this paper EAACK (ECDSA) significantly reduces the network overhead.

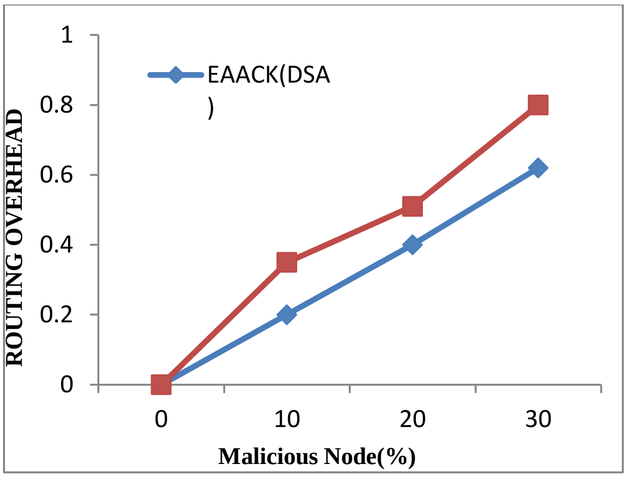

Fig.2 Routing Overhead

5.2Packet delivery ratio

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. When the malicious node increased, packet delivery ratio gradually decreased. It is due to the fact that more malicious nodes demand a lot more recognition packets and digital signatures.

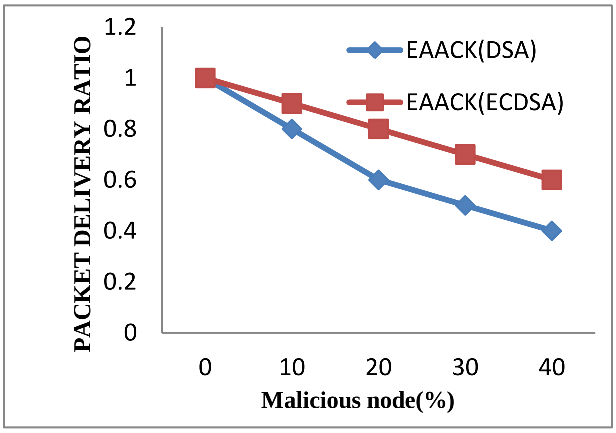

Fig.3 Packet Delivery Ratio

5.3 Total energy consumption

Total energy consumption metric in EAACK instance the total amount of energy consumed by each node in the network. When number of nodes in MANET increases, the energy consumption each node addition due to the fact that a lot more acknowledgement packets and digital signatures.The Fig. 4 shows an EAACK (ECDSA) significantly trim the energy consumption of each node in MANETs.

5.4 Inter arrival packet time ratio

Inter arrival packet time metric in EAACK is the time taken by the packet to reach the destination node from the source node. When the number of malicious node, the inter arrival packet time increase. The Fig. 5 shows that the proposed scheme execute better than EAACK (DSA) when malicious node is 20% and 30%,.

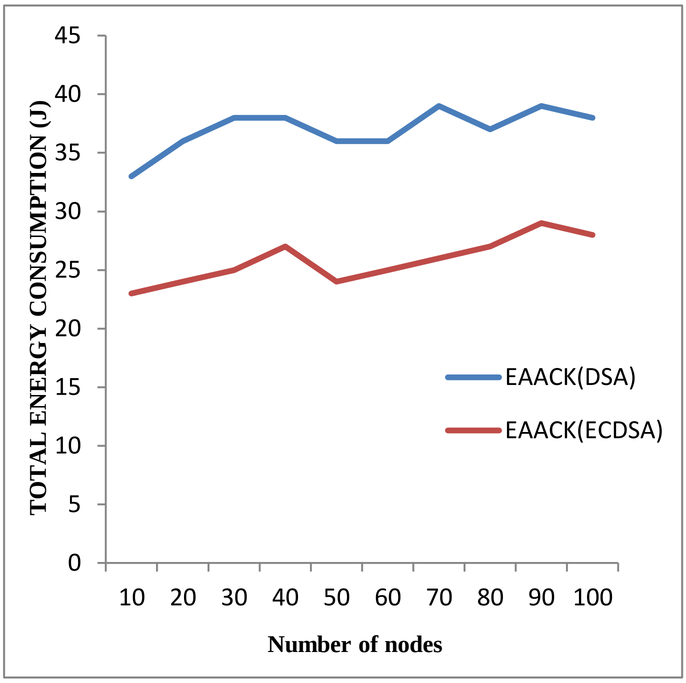

Fig.4 Total Energy Consumption

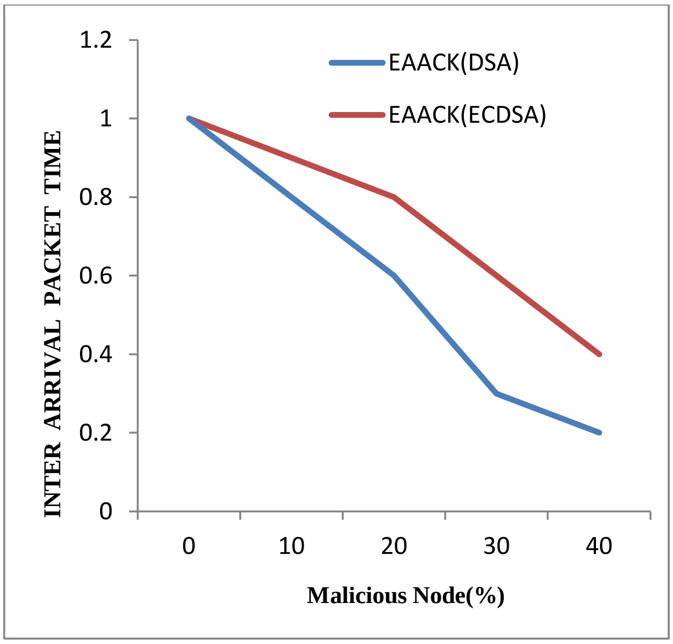

Fig.5Inter arrival packet time

6. CONCLUSIONS AND FUTURE WORK:

Packet-dropping attack has always been a major menace tothe security in MANETs. In this research paper, suggested a novel IDS named EAACK protocol specially intentionalfor MANETs and compared it against other popularmechanisms in different scenarios through simulations. Theresults demonstrated positive performances against false misbehavior report.Furthermore, an effort to prevent the attackers from originatingcounterfeitacknowledgment attacks.

Eventually, this paper hasconcluded that theECDSA scheme is more suitable to be implemented in MANETs.To increase the merits of research work,

This paper can be investigated the following issues in the future research:

- Possibilities of adopting hybrid cryptography techniquesto further trim the network overhead caused by digitalsignature;
- Examine the possibilities of adopting a key exchangemechanism to eliminate the requirement of redistributedkeys;
- Testing the performance of EAACK in real network environmentinstead of software simulation.

7. REFERENCES:

[1] Akbani, E.Korkmaz, T., and Raju, G. V. S. 2012 Mobile Ad hoc Network Security In *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag.

[2] Akbani R.H, Patel,S and Jinwala,D.C.2012 DoS attacks in mobile ad hoc networks: A survey. In Proceedings of the*2nd Int. Meeting ACCT*, Haryana, India

[3]Anantvalee, Tand Wu, J.2008A Survey on Intrusion Detection in Mobile Ad Hoc Networks in*Wireless/Mobile Security*. New York: Springer- Verlag.

[4] Botan, A Friendly C++ Crypto Library. [Online]. Available: http:// botan.randombit.net/.

[5] Buttyan, Land Hubaux, J.P.2007*Security and Cooperation in WirelesNetworks*. Cambridge, U.K.: Cambridge Univ. Press.

[6] Jayakumar,G and Gopinath,G.2007 *Ad hoc* mobile wireless networks routing protocol—A reviewIn Proceedings of the INJ. *Computer Science*.[7] Johnson,D and Maltz,D.1996 Dynamic Source Routing in *ad hoc* wireless networks in *Mobile Computing*.

[7] Kang, N., Shakshuki, E and Sheltami,T. 2010 Detecting misbehaving nodes in MANETs.In Proceedings of the*12th Int. Conf.* Paris, France.

[8] Kang, N., Shakshuki, E and Sheltami, T.2011Detecting forged acknowledgements in MANETs In Proceedings of the*IEEE 25th Int. Conf. AINA*, Biopolis, Singapore.

[9] Lee J.S. 2008 A Petri net design of command filters for semiautonomous mobile sensor networks in *IEEE Trans. Ind. Electron*.

[10] Liu, K. Deng, J P. Varshney, K and Balakrishnan, K.2007 An acknowledgment-based approach for the detection of routing misbehavior in MANETs in *IEEE Trans. Mobile Comput*er.

[11] Marti,S., Giuli,T.J.,Lai,K and Baker,M.2000 Mitigating routing misbehavior in mobile ad hoc networks In Proceedings of the *6th Annu. Int. Conf. Mobile Compute. Newt*, Boston.

[12] Nasser, N and Chen, Y.2007 Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network In Proceedings of the *IEEE Int.Conf. Communication*, Glasgow, Scotland.

[13] Rivest, R., Shamir, A and Adleman, L.1983 A method for obtaining digitalSignatures and public-key cryptosystems in *Commun. ACM*,

[14] Sheltami, T., Al-Roubaiey, A., Shakshuki, E., and Mahmoud, A. 2009 Video transmission enhancement in presence ofmisbehaving nodes inMANETs In Proceedings of the*Int. J. Multimedia System*.

[15] Sun, B.2004 Intrusion detection in mobile ad hoc networks in Texas A&M Univ., College Station.

[16] Digital Signature Standard (DSS).2009 in Federal Information Processing Standards Publication, Gaithersburg, MD.

[17] Sharmila Begam, U and Murugaboopathi, G. 2013.A Recent Secure Intrusion Detection System for MANETS, International Journal of Emerging Technology and Advanced Engineering.

[18] Sheltami, R., Shakshuki, M and Nan Kang.2013 EAACK- A Secure Intrusion Detection System for MANETs. IEEE Transactions on Mobile computing.

[19] Tmote Skyin TIK WSN Research Group, The Sensor Network Museum— [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky