International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

METHOD OF INTRUSION DETECTION USING ENHANCED ADAPTIVE ACKNOWLEDGEMENT(EAACK)

J.HARSHA CHARAN[#1] , Dr.T.PEER MEERA LABBAI[*2],
[#] *J.HARSHA CHARAN(M.Tech),Dept of Computer Science and Engineering.SRM University,CHENNAI*
[*]*Dr.T.PEER MEERA LABBAI,Asst Prof, Dept of Computer Science and Engineering.SRM University,CHENNAI*

[1]*harshacharanreddy@gmail.com*
[2] peermeera69@gmail.com

***Abstract*—** The migration to wireless network from wired network has been a global trend in the past few decades.The mobility and scalability brought by wireless network made it possible in many applications.Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages.The self-configuring ability of nodes inMANETmade it popular among critical mission applications like military use or emergency recovery. However,open medium and wide distribution of nodes make MANET vulnerable to malicious attackers.In this case,it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.With improvements of technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend,we strongly believe that it is vital to address its potential security issues.In this paper, we propose and implement new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs.

Index terms - MANET,NODES,EAACK.

I. INTRODUCTION

Due to their natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more references over wired networks in the past few decades. Manuscript received March 3, 2011; revised November 6, 2011 and February 26, 2012; accepted March 29, 2012. Date of publication April 26, 2012; date of current version October 16, 2012. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by the Research and Graduate Studies of Acadia University, King Fahd University of Petroleum and Minerals (KFUPM), and King Abdulaziz City for Science and Technology (KACST), Saudi Arabia, for the support provided under Project #AR-29-71. E. M. Shakshuki is with the Jodrey School of Computer Science, Acadia University, Wolfville, NS B4P 2R6, Canada (e-mail: elhadi.shakshuki@ acadiau.ca). N. Kang was with the Jodrey School of Computer Science, Acadia University,Wolfville, NS B4P 2R6, Canada. He is now with 2nd Act Innovations Inc., Halifax, NS B3J 3J6, Canada (e-mail: 090331k@acadiau.ca). T. R. Sheltami is with the Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dharan 31261, Saudi Arabia(e-mail: tarek@kfupm.edu.sa). Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org. Digital Object Identifier 10.1109/TIE.2012.2196010 By definition, 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 [35]. 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

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

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 [10], [27], [29]. 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 [19], [30]. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14], [28]. 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 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 [1]–[3], [6]–[9], [15], [16], [22], [24], [26], [29]–[31]. In the next section, we mainly concentrate on discussing the background information required for understanding this research topic.

II RELATED WORK

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 [27]. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) [25].

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 [15], [20], [21], [25]. Nevertheless, as pointed out by Marti et al. [17], 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 in Section III.

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. [16] is one of the most important approaches among them. On

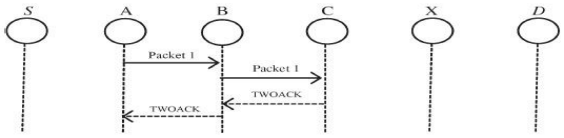

Fig. 1. TWOACK scheme:

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

Each node is required to send back an acknowledgment packet to the node that is two hops away from it. 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) [11]. The working process of TWOACK is shown in Fig. 1: 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 [25], [28], [29]. 3) AACK: Based on TWOACK, Sheltami et al. [25] 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 is shown in Fig. 2. In the ACK scheme shown in Fig. 2, 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 Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node. 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 [18]. 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 book [30] in 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 non repudiation [18]. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non repudiation 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 [33]. 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) [33].

2) Digital signature with message recovery: This type of scheme does not require any other information besides the

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

signature itself in the verification process. Examples include RSA [23].

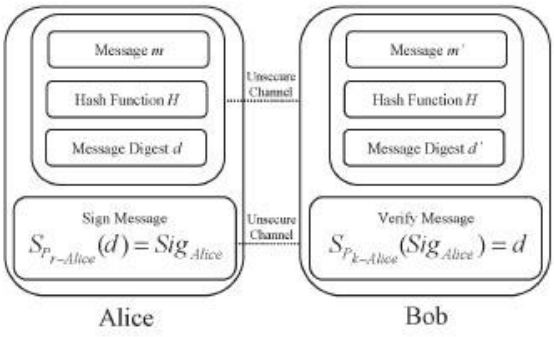

Fig. 3. Communication with digital signature.

In this research work, we implemented both DSA and RSA in our proposed EAACK scheme. The main purpose of this implementation is to compare their performances in MANETs. The general flow of data communication with digital signature is shown in Fig. 3. First, a fixed-length message digest is computed through a preagreed hash function H for every message m. This process can be described as H(m) = d. (1) Second, the sender Alice needs to apply its own private key Pr−Alice on the computed message digest d. The result is a signature SigAlice, which is attached to message m and Alice's secret private key

SPr−Alice (d) = SigAlice. (2)

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key Pr−Alice as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network. Next, Alice can send a message m along with the signature SigAlice to Bob via an unsecured channel. Bob then computes the received message m_ against the preagreed hash function H to get the message digest d_. This process can be generalized as

H(m') = d'.

Bob can verify the signature by applying Alice's public key Pk_Alice on SigAlice, by using

SPk−Alice (SigAlice) = d. (4)

If d == d_, then it is safe to claim that the message m_ transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

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.

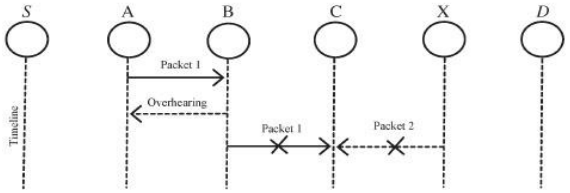

Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

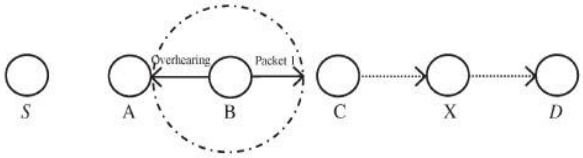

Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

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 [12], 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 [11], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I.Fig. 7 (shown later) presents a flowchart describing

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

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 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 time period, 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.

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. As shown in Fig. 9, 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 Psad1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 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 knowledge base and compares if the reported packet was received. If it is 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. With regard to this urgent concern, we incorporated digital signature in our proposed 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 [33] and RSA [23] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

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.

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 packet dropping 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. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

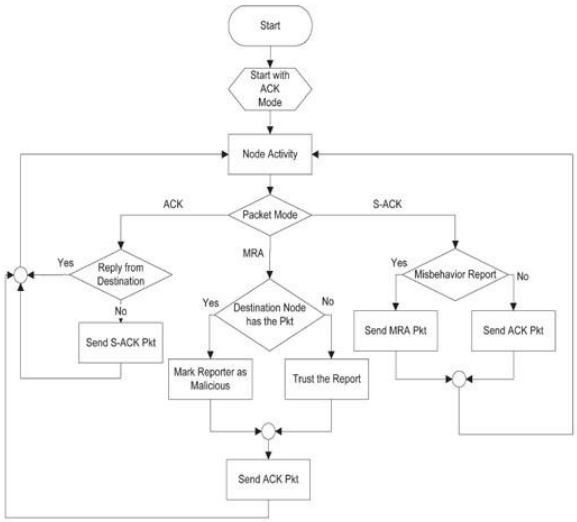

Fig. 9. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

B. Simulation Configurations Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 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 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, we ran every network scenario three times and calculated the average performance. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics [13].

1) Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2) Routing overhead (RO): 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]. During the simulation, 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 message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message. Regarding the digital signature schemes, we adopted an open source library named Botan [32]. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA and RSA schemes, we generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. We 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 and RSA are 89 and 131 B, respectively. In terms of

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

computational complexity and memory consumption, we did research on popular mobile sensors. According to our research, one of themost popular sensor nodes in themarket is Tmote Sky [34]. This type of sensor is equipped with a TI MSP430F1611 8-MHz CPU and 1070 KB of memory space. We believe that this is enough for handling our simulation settings in terms of both computational power and memory space.

TABLE I
PACKET TYPE INDICATORS

Packet Type	Packet Flag
General Data	00
ACK	01
S-ACK	10
MRA	11

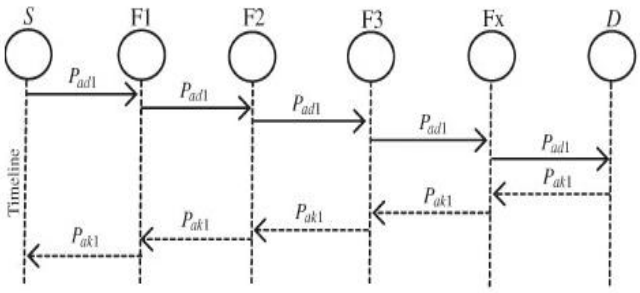

Fig. 6. System control flow: This figure shows the system flow of how the EAACK scheme works.

Data Encryption: When a sender wants to deliver its confidential data *M*, he defines the tree access structure *T* over the universe of attributes *L*, encrypts the data under *T* to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm chooses a polynomial q_x for each node *x* in the tree *T*. These polynomials are chosen in a top down manner, starting from the root node *R*. For each node *x* in the tree *T*, the algorithm sets the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node. For the root node *R*, it chooses a random $s \ Z^*_p$ and sets $q_R(0) = s$. Then, it sets d_R other points of the polynomial q_R randomly to define it completely. Let *Y* be the set of leaf nodes in the access tree. To encrypt a message *M* G_1 under the tree access structure *T*, it constructs a cipher text *(CT)* using public keys of each authority as given in equation

IV DATA DECRYPTION

When a user receives the cipher text *CT* from the storage node, the user decrypts the cipher text with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm *DecryptNode (CT, SK, x)* that takes as inputs a cipher text *CT*, a private key *SK*, which is associated with a set of attributes, and a node *x* from the tree *T*. It outputs a group element of *G*. The *DecryptNode (CT, SK, x)* algorithm is given by equation 2.

$$DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$$

The decryption algorithm begins by calling the function on the root node *R* of the access tree. We observe that $DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$ if the tree *T* is satisfied by . When we set $A = DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$, the algorithm decrypts the cipher text by computing *M*.

REFERENCES

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

[2] **D.Johnson and D.Maltz, "Dynamic Source Routing in *ad hoc* wireless networks**," in *Mobile Computing*. Norwell, MA: Kluwer.

[3] **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.*.

[4] **V.C.Gungor and G.P.Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach**," *IEEE Trans. Ind.Electron.*.

[5] **Y.Hu, D.Johnson, and A.Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks**," in *Proc. 4th IEEEWorkshopMobile Comput. Syst. Appl.*,

[6] **K.Al Agha, M.-H.Bertin, T.Dang, A.Guitton, P.Minet, T.Val, and J.-B.Viollet, "Which wireless technology for industrial wireless sensornetworks? The development of OCARI technol**," *IEEE Trans. Ind. Electron.*.

[7] **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.

[8] **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.,

[9] **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.

[10] **G.Jayakumar and G.Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review**," *J. Comput. Sci.*, vol 3.,

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-086 PAGE NO: 491-498.

[11] **L.Buttyan and J.P.Hubaux, "*Security and Cooperation in Wireless Networks*".** Cambridge, U.K.: Cambridge Univ. Press.,
[12] **N.Kang, E.Shakshuki, and T.Sheltami**, "**Detecting forged acknowledgements in MANETs**," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis,Singapore.
[13] **K.Kuladinith, A.S.Timm-Giel, and C.Görg**, "**Mobile *ad-hoc* communications in AEC industry,**" *J. Inf. Technol. Const.*,.
[14] **J.-S.Lee**, "**A Petri net design of command filters for semiautonomous mobile sensor networks**," *IEEE Trans. Ind. Electron.*
[15] **A.Tabesh and L.G.Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator**," *IEEE Trans. Ind. Electron.*,