ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

A Secure Acknowledgement Based Intrusion Detection System for Misbehaving Links in MANET

Harshavardhan [1], Dr.Balasubramani R [2]

Research Scholar, Dept. of Computer Science, NMAMIT, Nitte, Karkala (T), Udupi (D), India.1

Professor & Head, Dept. of Information Science, NMAMIT, Nitte, Karkala (T), Udupi (D), India. [2]

ABSTRACT: The term "ad hoc" implies that this network is a network established for a special, often extemporaneous service adapted to applications. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. MANET do not have fixed infrastructure. Because of its open medium and dynamic topology MANET is vulnerable to malicious attackers. Providing security against the intruder is a challenging task in MANET. It is proposed [1], that Enhanced Adaptive Acknowledgement (EAACK) a new intrusion detection system can be used to diminish MANET from attacks. RSA and DSA algorithms are used to authenticate the acknowledgement packets used in the proposed technique in order to improve the security level. It detects malicious misbehavior links more efficiently. In this paper we provide an implementation for the above mentioned approach.

KEYWORDS: MANET; Digital Signature, DSA, RSA, EAACK

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of autonomous mobile nodes that communicate with each other via wireless link over a range of bandwidth and equipped with both a wireless-transmitter and receiver. One of the major compensation of wireless networks is its ability to maintain their mobility after the communication of data between different sources. However, the communication is possible in the bandwidth range of transmitters. This means that two nodes cannot communicate with each other when they are away from the communication range. This dilemma is solved by MANET by allowing the in-between parties to relay data transmissions. For this purpose, MANET is divided into two types of networks, namely, single-hop and multi-hop. In a single-hop network, all nodes that are in the same bandwidth range communicate directly with each other. Whereas, in a multi-hop network, if the destination node is out of its bandwidth range then the nodes will depend on other in-between nodes to transmit. In converse to the traditional wireless network, MANET has no fixed network infrastructure. Thus in MANETs, all nodes are free to move arbitrarily [22], [23], [24]. The operation of MANETs does not depend on pre-existing infrastructure or base stations. MANET creates a self-configuring and self-maintaining network without the help of a centralized infrastructure. MANET is often infeasible in mission critical applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET is used in situation where a suitable infrastructure is not available or is impossible to install. It is mainly used in situations like natural or human-induced disasters, military conflicts and medical emergency situations [19], [30].Since the MANET is widely used in mission critical applications, network security is of vital importance. Compared to wired networks, MANET are vulnerable to various types of attacks because to the open medium and dynamic node distribution. For example, the malicious attacker can easily capture and compromise nodes to achieve attacks due to the lack of physical protection among nodes. Most routing protocols in MANET assume that all nodes in the network cooperatively maintain connectivity with other nodes and assuming that no malicious [7] attackers can easily compromise MANET by inserting malicious or non-cooperative nodes into the network.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

II. RELATED WORK

The limitations of most MANET routing protocols is that the nodes in MANET 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, Intrusion Detection System (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 first time. IDSs usually act as the second layer in MANET [22]; we mainly describe three existing approaches, namely, Watchdog [11], TWOACK [27] and AACK [14].

A. Watchdog

The aim of the watchdog scheme is to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Path rater. The purpose of Watchdog scheme is that it serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by carefully listening to its next hop's transmission. If the next node fails to forward the packet within a certain period of time, watchdog increases its failure counter. Watchdog node reports it as misbehaving if a node's failure counter exceeds a pre-defined threshold. In this case, to avoid the reported nodes in future transmission, the Path rater cooperates with the routing protocols.In the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power,4) false misbehavior report, 5) collusion, and6) partial dropping Watchdog scheme fails to detect malicious misbehaviors [11].

B. TWOACK

With respect to the six weaknesses of Watchdog scheme, by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination, TWOACK detects the misbehaving links. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement 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. The receiver collision and limited transmission power problems posed by Watchdog is successfully solved by TWOACK scheme.

C. AACK

A new scheme called Adaptive ACKnowledgement (AACK) was proposed based on TWOACK scheme. Similar to TWOACK, AACK is an acknowledgement-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK.

III. DIGITAL SIGNATURE

Digital signature is a mechanism used to protect the integrity of the information. Digital signature is an integral part of cryptography. Cryptography is a practice and techniques for secure communication in the presence of the third parties. In general, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [15]. The security in MANETs is defined as combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. 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 origination entity [17]. Digital signature schemes can be mainly divided into the following two categories:

1. Digital Signature: In the signature verification algorithm, the original message is required. Example: Digital Signature Algorithm (DSA) [17].
2. Digital Signature with Message Recovery: This type of scheme requires the signature itself in the verification process and no other information is required. Example includes RSA [16].The general flow of data communication with digital signature is as shown in fig2.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

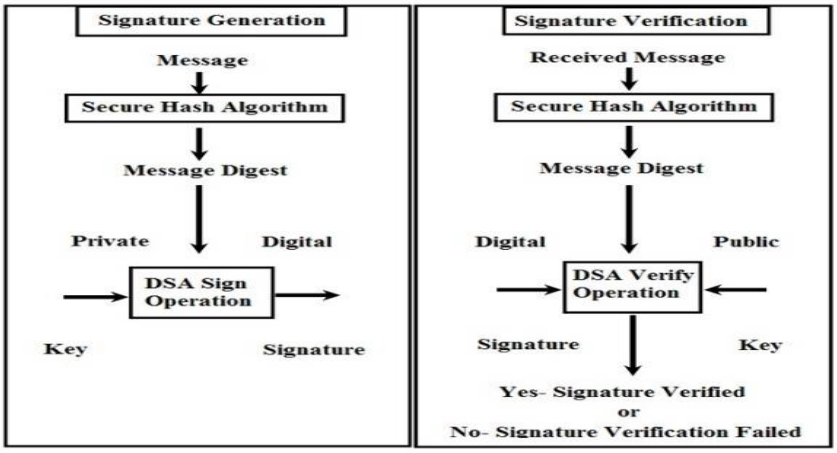

Figure 1: Communication with digital signature

IV. METHODOLOGY

The proposed approach [1] in EAACK can help to avoid three of the weaknesses of Watchdog method. They are: false misbehavior, limited transmission power and receiver collision. Here we implement these three weaknesses. EAACK mainly constituted of three major parts. They are: ACKnowledge (ACK), Secure-ACKnowledge (S-ACK) and Misbehavior Report Authentication (MRA).

A. ACK

ACK is an end-to-end acknowledgement method. It is the basic approach in EAACK, for reducing network overhead in times where there are no misbehavior in network.

B. S-ACK

S-ACK [12] method is similar to TWOACK with some added security. Here as proposed, each three consecutive nodes will work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The introduction of S-ACK is mainly to find the misbehaving in the presence of receiver collision or limited transmission power.

C. MRA

The Misbehavior Report Authentication (MRA) method is implemented to solve some of the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report could be generated by malicious attackers that report few of the regular working nodes as malicious, which is a false report and must be corrected. This kind of report can be misleading and can damage to the entire network thus cause a network division by breaking down the sufficient nodes required for transmission. The center of MRA approach is to check whether the destination node has received the reported missing packet through a different route.To start with MRA mode, the source node will first search its local knowledge base and seek for alternative route to the destination node. If there are no other route exists, then source node will start a DSR routing request to find new route to destination node. Because of this nature of MANETs, it is common to find multiple routes between any two nodes.

V. IMPLEMENTATION

The EAACK scheme is implemented by using the algorithms like DSA [17] and RSA [16] with the introduction of Digital signature with RSA is used to prevent the attackers from forging acknowledgement packet. The EAACK scheme requires all the acknowledgement packets to be digitally signed before they are sent out and verified until they

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

are accepted and extra resources are required with the introduction of digital signature in MANETS, the security of DSA is high and more efficient.

A. Digital Signature Algorithm

Digital signatures are essential is used to verify the sender of a document's identity. A digital signature is represented in a computer as a string of binary digits. The signature is computer using a set of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be verified. The signature is generated by the use of a private key. A private key is known only to the user. The signature is verified makes use of a public key which corresponds to the private key. With every user having a public/private key pair, this is an example of public-key cryptography. Public keys, which are known by everyone, can be used to verify the signature of a user. The private key, which is never shared, is used in signature generation, which can only be done by the user. The DSA algorithm procedure can be explained as

1. DSA Key Generation
The DSA key generation steps are as follows

Step 1: Firstly shared global public key values (p, q, g) are chosen:
Step 2: Choose a large prime p=2L Where L=512 to 1024 bits and is a multiple of 64.
Step 3: Choose q, a 160 bit prime factor of p- 1
Step 4: Choose g=h (p-1)/q for any h<p-1, h (p-1)/q (mod p)>1
Step 5: Each user chooses a private key and computes their public key:
Choose x<q, compute y=gx (mod p)

2. DSA Signature Creation and Verification
The DSA signature creation and verification steps are as follows

Step 1: To sign a message M Generate random signature key k, k<q compute
- $R=(g^k(\text{mod } p))(\text{mod } q)$
- $S=k^{-1}$ SHA (M)+x.r(mod q) Send signature (r ,s) with message.

Step 2: To verify a signature, compute
- $w= s^{-1}(\text{mod } q)$
- u1=(SHA(M).w)(mod q)
- u2=r. w(mod q)
- v=(gu1.yu2(mod p))(mod q) if v=r then the signature is verified

B.RSA

The RSA Algorithm (named after its inventors Rivest, Shamir and Adleman) is a widely used for public key cryptography. Based on exponentiation in a finite (Galois) field over integers modulo a prime number. Exponentiation takes O((log n)3) operations. Uses large integers (eg. 1024 bits).Security due to cost of factoring large numbers nb. Factorization takes O (e log n log log n) operations.
The RSA algorithm steps are as follows.

Step 1: Each user generates a public/private key pair by selecting two large primes at random p,q
Step 2: Computing their system modulus N=p.q, Where z(N)=(p-1)(q-1)
Step 3: Selecting at random the encryption key e, Where1<e<z(N), gcd(e,z(N))=1
Step 4: Solve following equation to find decryption key d e.d=1 modz(N) and 0<=d<=N
Step 5: Publish their public encryption key: KU={e,N},Keep secret private decryption key: KR={d,p,and q}
Step 6: To encrypt a message M the sender obtains public key of recipient KU={e,N}
-Computes: C+ Me mod N, where0<=M<N
Step 7: To decrypt the cipher text c:uses their private key KR={d,p,q} computes: M=Cd mod N

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

VI. RESULTS

This chapter deals the results of the EAACK scheme with the use of key properties of DSA with RSA for the encryption of data and authenticating the acknowledgement packets and explains the results with the help of snapshots as shown in proceeding steps.

A. Results and Discussions

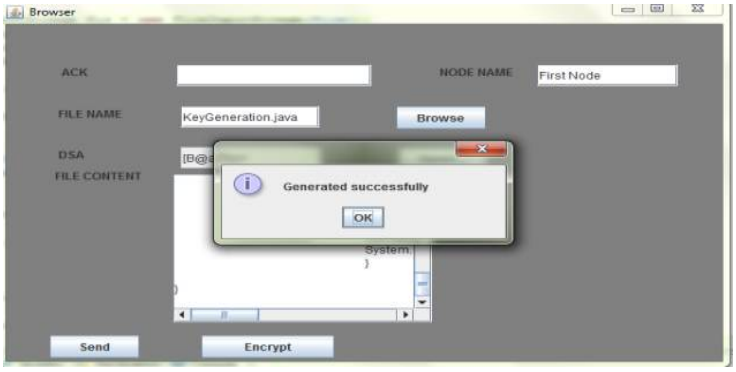

Figure 2: Source node generates DSA key

In the figure 2 the source node generates the DSA with RSA key while sending the data to intermediate node. The key will be used for the encryption of data from the source node to the intermediate nodes.

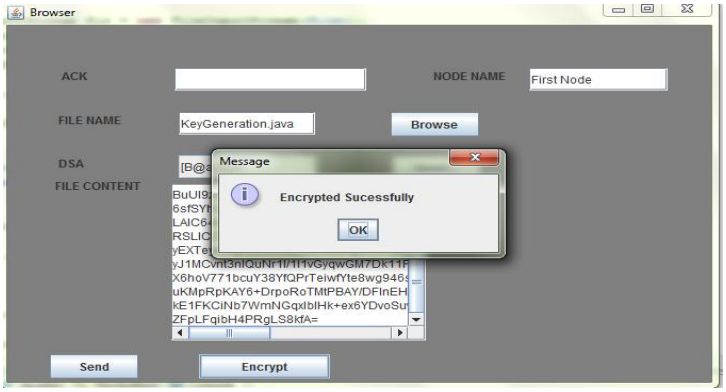

Figure 3: Source node encrypt the data

Figure 3 shoes that after generating the keys the source node encrypt the data and send the data to destination. The keys generated using the DSA and RSA will be used for the encryption.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

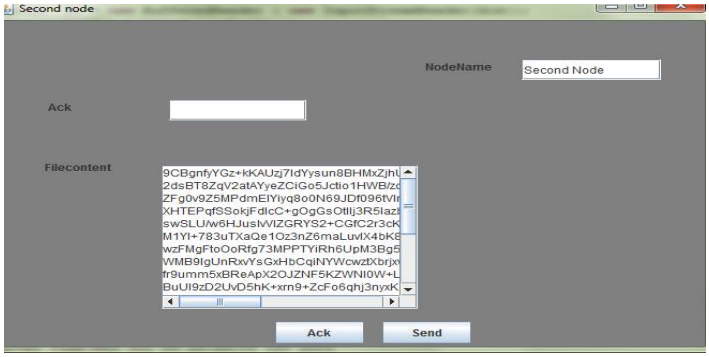

Figure 4: The intermediate node contains data

As shown in the figure 4, the intermediate node receives the file contents from the source node and this data sent to the destination node. The intermediate node is not having any idea about what the file contains because the data is being encrypted by the source node.

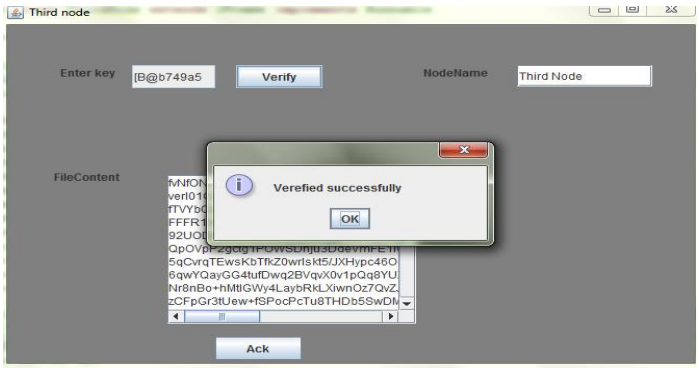

Figure 5: Destination node verifies the key

Figure 5 states that destination node receives the data from source that contents of the data to be verified through the DSA key. The receiver node uses the public key of the sender to verify the signature using the DSA algorithm.

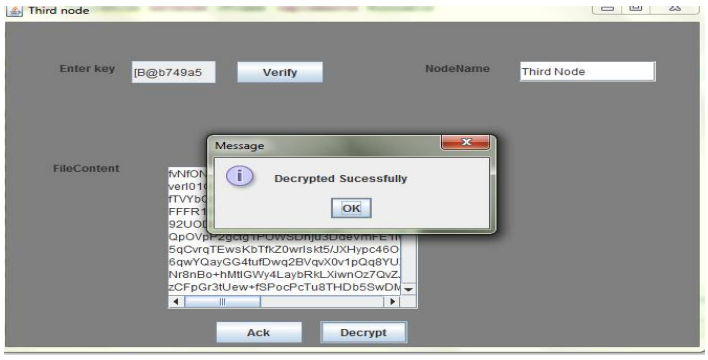

Figure 6: Destination node decrypts the data

In the figure 6 shows that the destination node receives the data from source and decrypts the contents of the data by using the DSA and RSA keys and sends back the acknowledgment to the source node. Upon verifying the signature the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

receiver node decrypts the data using the key and get to see the contents of the file after which the receiver node sends back the acknowledgement to the sender through the intermediate nodes.

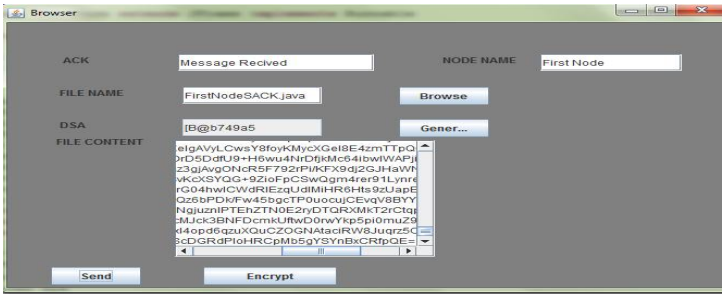

Figure 7: Source node receives Ack from destination

In the figure 7 states that source node receives the Ack from destination without fail of any data. This ensures the successful secure transmission of data from source to destination and the successful secure transmission of acknowledgement from destination to source.

VII. CONCLUSION AND FUTURE WORK

Mobile Ad-hoc network is the active research area that is being wide spread due to lot of application in military and civilian communication. This kind of network asks for cooperation of all its members in networking function, which makes it vulnerable to attacks. This intern affects the routing. The misbehaving nodes participating in network Route Discovery phase can cause severe degradation as per performance of the network as they refuse to forward the data packets. In this paper, we studied some of the problems faced in terms of security for MANETs. Also we have implemented the proposed approach called EAACK, which is specifically designed for MANETs. The evaluation of its performance with respect to existing system such as watchdog, TWOACK and AACK shows drastic improvement and overcomes its weaknesses like receiver collision, limited transmission power and false misbehavior report.

To increase the merits of the research work, we are planning to investigate the following issues in our future research:
1. Possibilities of adopting hybrid cryptography techniques to reduce the network overhead caused by digital signature.
2. Examine the possibilities of adopting key exchange mechanism to eliminate the requirement of pre-distributed keys.
3. Testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE “EAACK—A Secure Intrusion-DetectionSystem for MANETs”, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
[2] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012.
[3] R.H. Akbani, S. Patel, D.C. Jinwala. “DoS Attacks in Mobile Ad Hoc Networks: A Survey”, the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012.
[4] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: SpringerVerlag, 2008.
[5] Y. Hu, D. Johnson and A. Perrig. “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”. In the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.
[6] R. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-key Cryptosystems” .In the Communications of ACM, vol. 21, pp. 120-126, 1978.
[7] L. Buttyan and J.P. Hubaux.Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.
[8] 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
[9] K. Al Agha, M.-H.Bertin, T. Dang, A. Guitton, P. Minet, T. Val, J.-B.Viollet, "Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technol," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4266-4278, Oct 2009.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

[10] 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.
[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
[12] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5,pp. 536–550, May 2007.
[13] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer,ch. 5,pp. 153–181,1996.
[14] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Videotransmission enhancement in presence of misbehaving nodes in MANETs,"Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
[15] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.
[16] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communication. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.
[17] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD,Digital Signature Standard (DSS), 2009.
[18] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.
[19] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Comput., Commun., 2004, pp. 747–752.
[20] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.
[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] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[23] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.
[24] 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., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[25] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int.Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
[26] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc.ACM Workshop Wireless Secur., 2002, pp. 1–10.
[27] 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.