IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

SRD-Ad: Secured Routing and Data Delivery using Anonymous Detection in wireless networks

S. Suganya M.E.[1], T. Sakthi Sree M.E.[2],

Kathir College of Engineering Coimbatore[1]

Assistant Professor, CSE Dept, Kathir College of Engineering Coimbatore[2]

Abstract: In wireless networks, the secure data communication is needed to collect data from source to destination. Collected data are transmitted in a path consisting of connected links. All existing end-to-end routing protocols propose solutions in which each link uses a pair-wise shared key to protect data. In this paper, we propose a novel design of secure data communication. And energy drain rate, relative mobility estimation to predict the route lifetime. But this has given a problem of network congestion and delay. In this paper, we investigate the Secured Routing and data delivery(SRD) between the source–destination pairs in wireless networks (WN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services. Manage the Anonymous node information in terms of its available resources, the employed incentive mechanism and the quality-of-service (QoS) requirements, and the other terms of their historical behaviors. In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, in this framework we used Random Key Pre-distribution (RKP) a security key management for secure path selection criterion is designed to select the most reliable and shortest path in terms of routing available resources.

Keywords: Wireless networks, Public-key cryptosystems, Key Pre-distribution, Mobile nodes, Secure Authentication.

1. INTRODUCTION

Wireless networks have been deployed in various applications to collect information from human body, battle fields, smart power grids, Interstate highways, etc. Sensors are subjected by their physical limitations on hardware, storage space, computational power, etc. Developing efficient solutions to protect information in sensor networks is a challenging task. User authentication and key establishment are two fundamental security functions in most secure communications. The user authentication enables communication entities to authenticate identities of their communication partners. After users being successfully authenticated, a key establishment enables a secret session key to be shared among communication entities such that all exchange information can be protected using this shared key.
Traditional communications are one-to-one type of communications which involves only two communication entities. Most existing user authentication schemes involve only two entities, one is the prover and the other one is the verifier. The verifier interacts with the prover to validate the identity of the prover.
As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks use wireless technology without a pre-existing infrastructure (access points). As the name states, It consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability.
In this proposed framework, we used SRDD-AD named Secured Routing and Data Delivery by Anonymous Detection in Wireless Sensor Networks We investigate the Secured Routing and data delivery between the source–destination pairs in wireless sensor networks (WSN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services. Manage the Anonymous node information in terms of its available resources, the employed incentive mechanism and the quality-of-service (QoS) requirements, and the other terms of their historical behaviors.
In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, a path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources.

2. RELATED WORKS

In previous many works, discussed and used key distribution and authentication schemes for secure data sharing and detect malicious nodes in networks. Now here we discuss some works for network detection and prevention.
An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANET, We are considering the Routing misbehavior in MANETs (Mobile Ad Hoc Networks). Routing protocols for MANETs are based on the assumption which are, all participating nodes are fully cooperative.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

One such routing misbehavior is that some nodes will take part in the Route discovery and maintenance processes but refuse to forward data packets. In this, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their effect. The basic idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path.

Secure Trace Route to Detect Faulty or Malicious Routing, Internet routing is vulnerable to disruptions caused by malfunctioning or malicious routers that draw traffic towards them-selves but fail to correctly forward the traffic. The existing approach to securing routing is to validate routing updates by verifying their authenticity, accuracy, and/or consistency.

Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing, In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. In this paper, while observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance. To improve the detection accuracy, we propose to exploit the correlations between lost packets.

Here presented a protocol for routing packets between wireless mobile hosts in an ad hoc network. Unlike routing protocols using distance vector or link state algorithms, our protocol uses dynamic source routing which adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

This proposed technique works as follows. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. If any of the routes responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

In the present studies it is proposed a novel scheme named Anonymous Detection which provides detect routing misbehavior and to overcomes their adverse effect. The performance of the schemes analyzed and simulated and 95% packet delivery ratio were achieved when 40% misbehaving nodes were present in the Wireless networks.

3. SYSTEM MODEL

Innovative techniques that improve energy efficiency to prolong the network lifetime are highly required. An effective topology control approach in wireless networks, which can increase network scalability and lifetime. In this paper, we propose a novel secure schema for wireless sensor networks, which better suits the periodical data gathering applications. Our approach elects nodes with more residual energy through local radio communication while achieving well data distribution. And this scheme is secure against adaptive chosen-message attacks.

Preventing or detecting malicious nodes launching collaborative attacks is a challenge. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the RKP (Random Key Pre-distribution) that integrates the advantages of both proactive and reactive defense architectures.

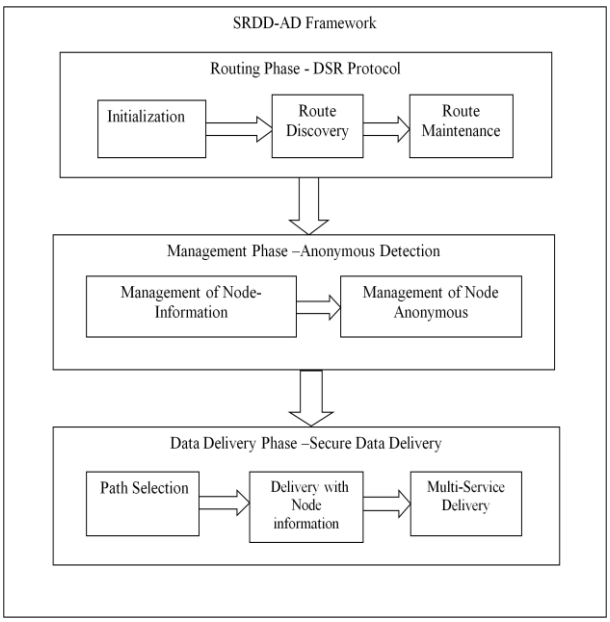


Fig.3.1 Architecture Design

DOI10.17148/IJARCCE.2017.6582

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

3.1 DSR Protocol
Overview and Important Properties of the Protocol The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network: Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D. 3 Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.
Route Discovery and Route Maintenance each operate entirely on demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network.

3.2 Anonymous Detection - Random Key Pre-Distribution
In this process the framework of random key pre-distribution to address the bootstrapping problem. First, we propose the random key pre-distribution scheme, which achieves greatly strengthened security under small scale attack while trading off increased vulnerability in the face of a large scale physical attack on network nodes. We will explain why this trade-off is a desirable one. Second, we present the multi-path key reinforcement scheme, which substantially increases the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising any given communication.

Finally, we propose the random-pair-wise keys scheme, which assures that, even when some number of nodes have been compromised, the remainder of the network remains fully secure. Furthermore, this scheme enables node-to-node mutual authentication between neighbors and quorum-based node revocation without involving a base station. Node-to-node mutual authentication here refers to the property that any node can ascertain the identity of the nodes that it is communicating with. We give a detailed analysis of each proposed scheme and show under which situations our schemes can be used to achieve maximum security.

4. PROPOSED MODEL

In this proposed framework, we used SRDD-AD named Secured Routing and Data Delivery by Anonymous Detection in Wireless Sensor Networks We investigate the Secured Routing and data delivery between the source–destination pairs in wireless sensor networks (WSN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services. Manage the Anonymous node information in terms of its available resources, the employed incentive mechanism and the quality-of-service (QoS) requirements, and the other terms of their historical behaviors. In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, a path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources.

4.1 Network Model
In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window (nam window). We have syntax for create nodes in network animator window. Then we can create nodes in two types like random and fixed motions.

In random motion we fixed range for X and Y, fixed particular range then the nodes are randomly generate in that range of nam window. In fixed motion we give X and Y dimension position for all nodes then all the nodes are fixed in that particular dimension.
Sensor nodes are aware of their own positions. The position information may be based on a global or a local geographic coordinate system defined according to the deployment area. Determining the position of the nodes might be achieved using a satellite based positioning system such as global positioning system (GPS) or one of the energy-efficient localization methods proposed specifically for MANETs.

Every sensor node should be aware of the position of its neighbors. This information enables greedy geographic routing and can be obtained by a simple neighbor discovery protocol. The coordinates of a network center point has to be commonly known by all sensor nodes. The network center does not have to be exact and can be loaded into the sensors' memories before deployment. The ring structure encapsulates the network center at all times, which allows access to the ring by regular nodes and the sink.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

4.2 Routing Scheme

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In this scheme, we are also going to use same method with different style, such as creating the fake route request. The source will generate fake request with destination address as cooperating neighbor.

Source already knows the information, for Freq no reply. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism. If route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is to store the neighbor information into table when it receives the beacon packet from the neighbor. Here fixed timer for all beacon messages, when neighbor got the beacon messages then send ACK to sender. If the time is got expire the neighbor node info will be deleted from the table.

4.3 Anonymous Detection

This proposed which integrates the Proactive and reactive defense architectures, and randomly establishing a cooperation with adjacent node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program.

Finally the detected malicious node is listed in the anonymous list and notifies the remaining nodes in the network to halt any communication with them. Because some of the traffic data are not reliable, it is critical to find an evidence combination technique to properly fuse together multiple pieces of evidence in presence of both trustworthy and untrustworthy data. Thus, it is necessary to combine multiple pieces of evidences so that both data trust and functional trust can be properly evaluated.

In this work, is used to fuse together multiple piece of evidences even if some of them might not be accurate. As a result, my proposed scheme can reduce packets loss that can be cause by malicious nodes and have better throughput.

4.3.1 Random Key pre-distribution

Generally, a key establishment scheme has nothing to do with the routing protocol. However, the path in lots of RKPD schemes, such as the basic scheme, is set up through a routing protocol. That is, a customized routing protocol needs to be used along with those key distribution schemes, which will seriously affect the portability of those RKPD schemes. Moreover, the number of hops of the path may increase because the adjacent nodes in the path must be logically connected.

Our scheme is less competitive in terms of the computation and communication complexity analysis. However, the execution time of a path key establishment for our scheme is slightly less than that of the basic scheme in the simulation. The reason is that, the complexity does not include the extra traffic and calculations that are caused by the customized routing protocol in the basic scheme.

The Scheme

A new random key pre-distribution scheme is described in this section. The scheme also includes three phases:

(1) Key pre-distribution,
(2) Shared key discovery, and
(3) Path key establishment.

Key pre-distribution: Before the deployment of nodes, for each node, a control center (CC) randomly chooses a key ring and loads it into the node. The CC randomly generates keys and assigns a unique key identifier to each; those keys and the corresponding identifiers compose a key pool.

The CC chooses a deterministic algorithm to decide the key identifiers allocated to each node on the input of the node's identifier. For each node, the CC inputs its identifier into and output distinct values between and, denoted by. At last, the CC draws keys whose key identifiers are. Those keys and the corresponding key identifiers compose a key ring which is loaded into node.

Shared key discovery: After the deployment of nodes, each node creates its own neighbor list. Each node broadcasts its identifier and records the received identifiers, denoted by. For each node, node runs the procedure and generates the key identifier set of nodes. If there is a common key identifier in such set and its own key ring, they are logically connected. Then node adds a record involving the node identifier and the same key identifier to its neighbor list.

Path key establishment: Node wants to establish a path key with node. If they are in wireless communication range and have a shared key, that is, they are on each other's neighbor list the shared key can be used as the path key. Else, randomly generates a path key and encrypts with some key in key ring. The cipher text, denoted by, together with the identifier of the encryption key is sent to on a physical connected path founded by a routing protocol. Finally, finds the encryption key corresponding to the received key identifier and decrypts CT to obtain. The following procedure explains how can find an encryption key which belongs to key ring.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

4.4 Data Delivery Phase

For delivering multi-services, the sources find some paths by virtue of the traditional routing protocol. Nevertheless, these paths may not be all reliable for successfully forwarding multi services due to the node-selfishness of the relay node within the paths. Although the relay node represents its behavior of forwarding multi-services, the sources should provide large incentives for stimulating the multi-service forwarding of these data and maintaining the reliability of the selected path. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack.

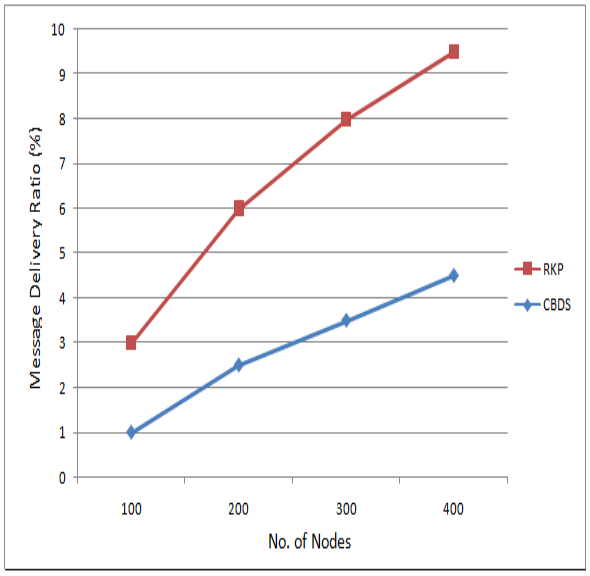
5 .PERFORMANCE ANALYSIS

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the network performance. All sensor nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes.

This study evaluates the following main performance metrics:

1) Message delivery ratio: is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.
2) Residual energy: measures the mean value of the residual energy of all alive sensor nodes when simulation terminates.
3) Delivery latency: means the time delay experienced by the source node while transmitting a report message to the sink.

Message Delivery Ratio:



Above graph compares the simulation results of message delivery ratios of the original Routing and RKP the message delivery ratios of this mechanisms decreases, as Ns increases. In this case, the discovered routing path is broken, and the secure mechanism must reconstruct the data structure. This reconstruction may lead to additional energy consumption of sensor nodes, thereby decreasing the packet delivery ratio.

Residual Energy:

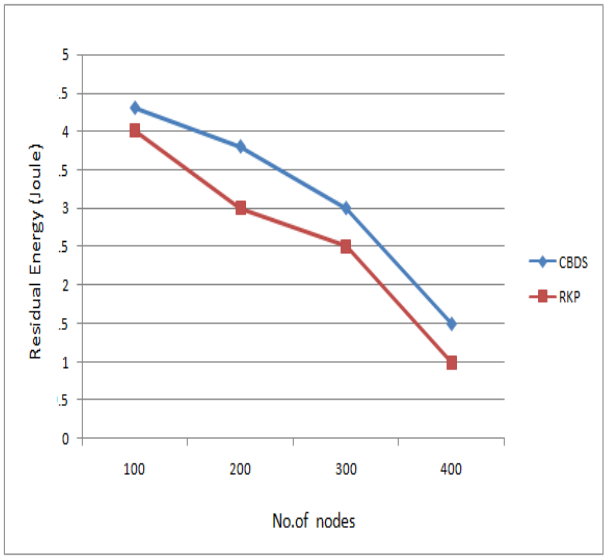
Following graph provides a comparison of the energy consumption results of four clustering mechanisms under scenarios with different nodes. In general, the clustering mechanism generates more clusters as the number of Ns increases. Sensor node consumes more energy in clustering thereby decreasing the residual energy.

Note that the increasing Node will increase the report frequency. Sensor nodes have to consume additional battery power to transmit the increased number of report messages. This leads to a reduction of the residual energy of the nodes in the network.

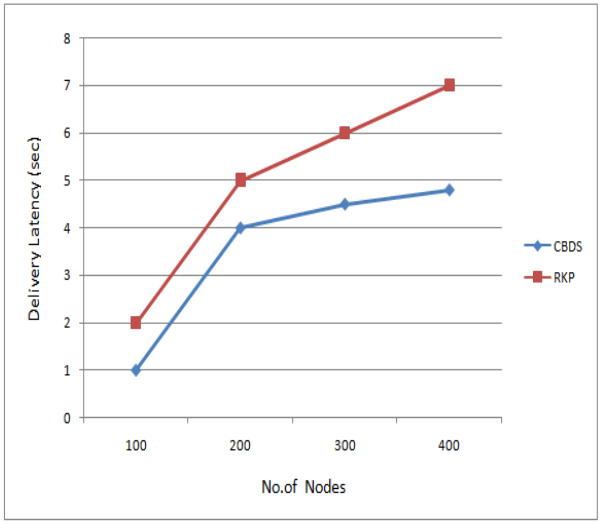
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017



Delivery Latency:



Above graph shows the average delivery latency of proposed RKP mechanisms under scenario with different N s and Nreq. As Ns increases, more data are generated and the length of the discovered routing path also increases. In securing, node death and poor link quality result in reconstruction of clusters and retransmission of report messages, respectively. The reconstruction and retransmission generate along message latency.

6. CONCLUSION

We developed SRD-Anonymous Detection, comprehensive misbehavior detection and mitigation system which integrates functions named: route discovery, detection of misbehaving nodes via keying security. We modeled the process of identifying misbehaving nodes as Key pre-distribution. We showed that SRD-AD recovers the network operation even if a large fraction of nodes is misbehaving at a significantly lower communication cost.

Moreover AMD can detect selective dropping attacks over end-to-end encrypted traffic streams. Under the Anonymous Detection management, in this framework we used Random Key Pre-distribution (RKP) a security key management for secure path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

REFERENCES

[1] G. Acs, L. Buttyan, and L. Dora, "Misbehaving router detection in link-state routing for wireless mesh networks," in Proc. IEEE Int. Symp. World Wireless Mobile Multimedia 2010,
[2] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless Ad Hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 11–35, 2008.
[3] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: Preventing selfishness in mobile Ad Hoc networks," inProc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.
[4] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors,"Commun. ACM, vol. 13, no. 7, pp. 422–426, 1970. [5] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile Ad-Hoc networks by reputation systems,"IEEE Commun. Mag., vol. 43, no. 7, Jul. 2005.
[6] L. Buttyan and J.-P. Hubaux, "Stimulating cooperation in selforganizing mobile Ad Hoc networks,"Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, 2003.
[7] J. Crowcroft, R. Gibbens, F. Kelly, and S. € Ostring, "Modelling incentives for collaboration in mobile Ad Hoc networks," in Proc. Workshop Model. Netw., 2003, pp. 427–439.
[8] A. Dhagat, P. Gacs, and P. Winkler, "On playing "twenty questions" with a liar," in Proc. 3rd Annul. ACM-SIAM Symp. Discrete Algorithms, 1992, pp. 16–22.
[9] Y. Dong, H. Go, A. Sui, V. Li, L. Hui, and S. Yiu, "Providing distributed certificate authority service in mobile Ad Hoc networks," in Proc. 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw., 2005, pp. 149–156.
[10] L. M. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an Ad Hoc networking environment," inProc. 20th Annu. Joint Conf. 2001,
[11] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks,"ACM Trans. SensorNetw., vol. 4, no. 3, pp. 1–37, 2008.
[12] K. Hansen, T. Larsen, and K. Olsen, "On the efficiency of fast RSA variants in modern mobile phones,"Int. J. Computer Sci. Inf. Security, vol. 6, no. 3, 2009, pp. 136–140.
[13] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for Ad Hoc networks," inProc. IEEE Wireless Commun. Netw. Conf., 2004
[14] D. Johnson, D. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multihop wireless ad hoc networks," In Ad hoc Netw., Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001, pp. 139–172.
[15] A. Jøsang and R. Ismail, "The beta reputation system," in Proc.15th Bled Electron. Commerce Conf., 2002, pp. 324–337.
[16] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures,"Ad Hoc Netw., vol. 1, no. 2/3, pp. 293–315, 2003.
[17] W. Kozma and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," inProc. 5th Int. ICST Conf. Security Privacy Commun. Netw., 2009, pp. 207–227.
[18] W. Kozma Jr. and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in Ad Hoc networks based on random audits," inProc. 2nd ACM Conf. Wireless Netw. Security, 2009, pp. 103–110.
[19] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets,"IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[20] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile Ad-Hoc networks," inProc. IEEE Wireless Commun. Netw., 2003, pp. 1510–1515.