Secured Routing with Respect to Trust and Keys in Wireless Sensor Network

Vishwa Patil[1] Shantala Devi Patil[2]
[1,2]Department of Computer Science & Engineering
[1,2]REVA ITM Visvesvaraya Technological University

Abstract— In the wireless sensor network, where in multi-hop routing provides least protection against identity fraud by replaying routing information. This type of defect can exploit to launch many types of harmful attacks like wormhole attacks, sinkhole attacks and Sybil attacks. This situation may be further aggregated with harsh mobile network condition. By using traditional cryptography techniques or developing some trust routing protocol does not effectively solve this problem. To provide secured routing solution for multi-hop routing in wireless sensor network need to design and implement secured and trust aware routing protocol for dynamic wireless sensor network, which does not require geographic information and time synchronization. Secured trust aware routing protocol (STRP) provides energy efficient and trustworthy routes and it also provide solutions against harmful attacks such as sinkhole, wormhole and Sybil attacks. The secured trust aware routing protocol is evaluated in both simulation and real time experiments on large scale wireless sensor network under various different scenarios.

Key words: Secured Trust Aware Routing Protocol (STRP), Trust Value, Energy Value, One Hop Neighbor

I. INTRODUCTION

Wireless sensor network these are ideally used for application purposes to detect events of interest such as forest fire monitoring and military surveillance. Wireless sensor network consists of battery powered sensor nodes with some limited processing capabilities. It also comprises a narrow radio communication range. Wireless sensor nodes sends the message to base station via multi-hop path or single hop, But in the multi-hop path routing of wireless sensor network often becomes the targets of malicious attacks. In these kind of situation attackers may create traffic collision, or may tamper nodes physically with valid transmission, or misdirect or drop message in routes. Attackers may also jam the channel by creating radio interference.

As in the multi-hop wireless sensor network there is chance of malicious attacks on nodes. An attacker may replays all the outgoing packets from the other valid node to forge the node identity. Then attacker node uses this forged identity and participate in network routing process thus disturbing the network traffic even if attacker node cannot directly receive the packets of valid node with the help of other attacker node it can receive the routing packets of valid node. This is known as wormhole attack.

In the wireless sensor network the attacker node steals the valid nodes identity and then replays to all the routing packets of the valid node thus attacker node misdirect the network traffic. The attacker node may drop the received packets or forward to other node which is not supposed to be in routing path or form a loop in the network, or break the network. The attacker node after stealing the valid node's identity sinkhole attack may be launched. The attacker node may claim itself as base station through replaying all packets from valid base station. Thus attacker claiming as base station, which is fake base station may create lot of traffic creating black hole. This same technique can be used to create another strong attack known as Sybil attack but here in this type of attack, the attacker may replay routing information in multiple nodes, as attacker may be present in multiple identity in the network

To protect the wireless sensor network by harmful attacks such as sinkhole, wormhole and Sybil attacks, to secure routing information need to design and implement robust secured routing with respect to trust and it assures the secured routing in wireless sensor network. Secured trust aware routing protocol doesn't required the geographic information or time synchronization. Even under strong attacks such as wormhole, sinkhole, or Sybil attacks the secured trust aware routing protocol provides stability in network performance. This secured trust aware routing protocol can be used with other protocol to provide security to other protocols. The main characteristics of the secured trust aware routing protocol is trust worthy and energy efficiency. Secured trust aware routing protocol can easily integrated into existing protocol with ease.

II. LITERATURE SURVEY

As sensor systems edge closer towards boundless organization, security issues turn into a focal concern. As such, much research has concentrated on making sensor systems plausible and valuable, and has not focused on security. We display a suite of security building squares upgraded for asset obliged situations and remote correspondence. Twists has two protected building squares: SNEP and TESLA. SNEP gives the accompanying imperative pattern security primitives: Data secrecy, two-gathering information verification, and information freshness. An especially hard issue is to give proficient telecast verification, which is an essential system for sensor systems. TESLA is another convention which gives confirmed telecast to extremely asset compelled situations. We executed the above conventions, and demonstrate that they are handy even on insignificant equipment: the execution of the convention suite effectively coordinates the information rate of our system. Also, we show that the suite can be utilized for building more elevated amount conventions.

One of the reasons that the exploration of interruption discovery in remote sensor systems has not progressed essentially is that the idea of "interruption" is not clear in these systems. In this paper we research inside and out a standout amongst the most serious assaults against sensor systems, in particular the sinkhole assault, and we underscore on methodologies that an assailant can take after to effectively dispatch such an assault. At that point we

propose particular discovery decides that can make real hubs get to be mindful of the danger, while the assault is as yet occurring. At long last, we show the assault and present some usage subtle elements that underscore the little exertion that an aggressor would need to put keeping in mind the end goal to break into a sensible sensor system.

Security is critical for some sensor system applications. An especially hurtful assault against sensor and impromptu systems is known as the Sybil assault, where a hub illegitimately asserts various characters. This paper methodically examines the risk postured by the Sybil assault to remote sensor systems. We exhibit that the assault can be exceedingly hindering to numerous essential elements of the sensor system, for example, directing, asset designation, mischief discovery, and so forth. We set up a grouping of diverse sorts of the Sybil assault, which empowers us to wager comprehend the dangers postured by every sort, and better plan countermeasures against every sort. We then propose a few novel strategies to guard against the Sybil assault, and break down their adequacy quantitatively.

III. EXISTING SYSTEM

In wireless sensor network most of routing protocol which are existing assumed to be honest nodes. Thus these protocol only focus on energy efficiency, and uses only the encryption of data for security purpose, so there are more chances of malicious attacks. Most existing directing conventions for WSNs either expect the genuineness of hubs and concentrate on vitality proficiency, or endeavor to bar unapproved investment by encoding information and verifying bundles. Cases of these encryption and validation plans for WSNs incorporate Spins, TinyPK, TinyECC and TinySec.

In addition to the cryptographic routines, trust and notoriety administration has been utilized in non-specific specially appointed systems and WSNs to secure directing conventions. Essentially, an arrangement of trust and notoriety administration appoints every hub a trust quality as per its past execution in steering. At that point such trust qualities are utilized to help choose a safe and proficient course. Be that as it may, the proposed trust and notoriety administration frameworks for nonexclusive specially appointed systems target just moderately effective equipment stages, for example, tablets and cell phones.

IV. PROPOSED SYSTEM

Wireless sensor network are protected from the harmful attacks utilizing the replay of routing information. Secured trust aware routing protocol is meant, to secure routing solutions in wireless sensing element in the networks.

Secured trust aware routing protocol is developed into an entire and freelance routing protocol, the aim is to permit existing routing protocols to include our implementation of Secured trust aware routing protocol with the smallest amount effort and so manufacturing a secure and economical fully-functional protocol.

V. SYSTEM DESIGN

The following figure shows detailed system design, where user need to choose the source node, then by using Euclidian algorithm one hop neighbor is found out. Then Optimal path is chosen between source and destination, then energy and trust values of nodes in optimal path are checked. Then packets are delivered to destination.

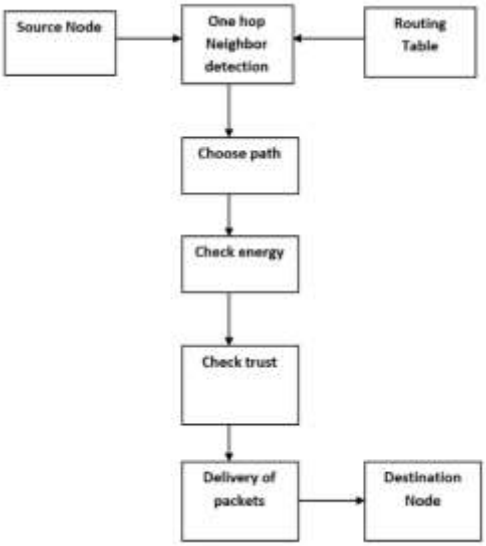


Fig. 1: Packets are Delivered to destination

Overall system can be divided into 5 modules as below

- Node deployment
- Multipath selection
- Route Selection
- Energy Watcher
- Trust Manager

A. Node Deployment

The proposed work considers Wireless Sensor Network with N nodes. Set of all nodes in the network is represented by N. With the sink as the root, all n nodes communicate using tree topology. In initial phase the tree is formed as follows. The sink node is a first node, which broadcasts a message with a hop counter. The receiving node after receiving a message from sender node, increase the hop counter by 1 and set the sender node as a parent node and broadcast the same message to their neighbors. Data flows along the edges in this communication tree topology.

Initially nodes are to be deployed in the network. The number of nodes to be deployed in the network must be defined correctly.

B. Multipath selection

A sensor network with a graph G(k)=(V(k),e(k)), where V(k) denotes node set that are active at time k and e(k) represents edge set which consists of (u,v) pairs of nodes such that nodes u and v can directly communicate between each other at time k. Active node represents that node participating actively, and has never failed permanently. Here Undirected graphs are considered in all cases, i.e., (i, j)=(j,i). The neighboring nodes of a node i is set as Ni, that are connected to i. "di(k)" represents the number of neighbors of i and it is called as i's degree.

A path from i to j is defined as a sequence of edges that are connecting i and j. If there exists a path between every pair of nodes then the graph is called connected graph. To transact a data, all the neighbor node of source node are considered and all the possible paths are found to reach the destination.

User must select both the source node and the destination node. While considering the multipath, all the neighbor nodes of source node are taken into account. Depending on the weight of links, shortest path among multipath are chosen. The route with the less weight, will be considered as the best route to transmit the data.

C. Route Selection

Considering both the trust worthiness and the energy efficiency, when secured trust aware routing protocol is enabled node N only needs to decide to which neighboring node it should forward the data packet, to route it to the base station. After the data packet is successfully transmitted to that next-hop node, the remaining task of delivering data to the base station is fully assigned to it, and N is totally unaware of the routing decisions made by the next hops and hence it maintains a neighborhood table with trust level values and energy cost values for few known neighbors.
When the source node is selected, user must also select the destination node. The neighbor nodes of the source nodes are taken into consideration while creating multi paths. Shortest path among the multipath is arrived using the weight between the links. The route, which is having less weight, will be taken as the best route to transmit the data.

D. Energy Watcher

For a node N, the energy cost of a neighbor is the average energy cost to successfully deliver a unit sized data packet to its neighbor as its next-hop node, from N to the base station. E is denoted as its energy cost. Numerically each and every node is provided with their own energy levels such as 1, 2, 3... Where 1 represents the lesser energy level compared to 2 and 3. Depending upon the energy levels assigned, the routing path is determined. The node, which acquires less energy, will be included in the route rather than the higher energy consumption.

User must select both the source node and the destination node. While considering the multipath, all the neighbor nodes of source node are taken into account. Depending on the weight of links, shortest path among multipath are chosen. The route with the less weight, will be considered as the best route to transmit the data.

E. Trust Manager

The trust worthiness of every neighbor node is a decimal number in [0, 1]. This represents N's opinion about trustworthiness level of neighbor. Specifically, the trust level of a neighbor node is decided by the node N depending upon the probability estimation of whether it successfully delivers the data to the base station correctly without compromising with the other malicious activities in the network. Trust value is provided to all the nodes in a network with the numerical values 0 or 1. Where 0 represents a malicious node and 1 represents the trust worthy node. T is represents the trust value assigned to every node. Based on this trust value the path is identified between the source node and the destination. Node with the trust value 1 is considered in the path and node with value 0 is eliminated from the secured path.

When the source node is chosen, user must select the destination node. The neighbor nodes of the source nodes are taken into consideration while creating multipath. Shortest path among the multipath is arrived using the weight between the links. The path is created based upon the trust value of the node.

F. Input Parameter for Solving Problems

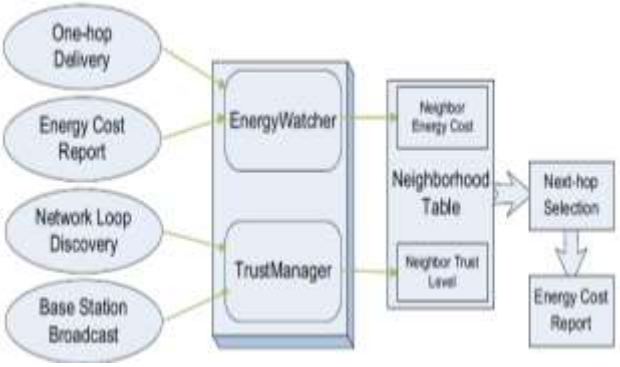


Fig. 2: Input Parameter

1) Neighbor Nodes

While identifying multiple paths, all the neighbor nodes of the source node are taken into consideration. For a -enabled node N, to transmit a data packet from source to Base station, N needs to determine only to which of the neighbor it can send the data successfully by checking both its trust worthiness and energy efficiency. Once the data is forwarded to next hop, the further forwarding of data packet to the base station is fully delegated to it. N is totally unaware of what routing decision the next hop makes.

2) Trust Value

That trust level is denoted by T. Each and every node is given a trust value wid an integer either 0 or 1. If the node is assigned with trust value 0, that node is considered as a malicious node and node with the trust value 1 represents the normal node. Depending upon the assigned trust value, the routing path is constructed. The node, which has trust value 1, will be included in the route, and the node having trust level 0 is not considered in selected path.

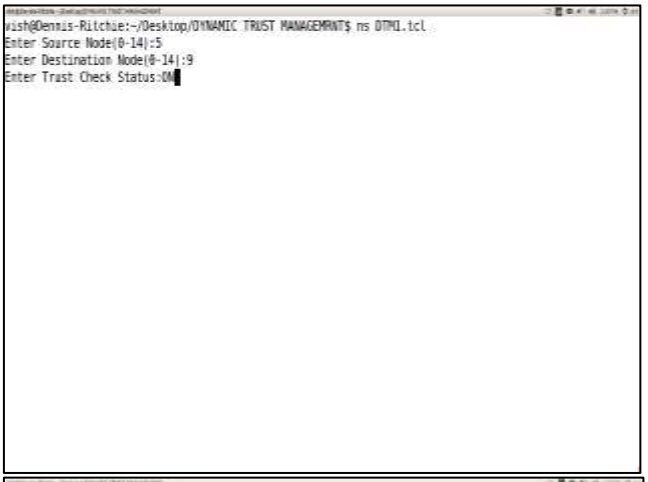
3) Energy Value

Energy value is denoted by E. Each and every node is assigned with their own energy values in terms of joules, the value is given as integers such as 1, 2, 3…, whereas 1 is considered to be less energy consumption rather than 2 or 3. Routing path is constructed depending upon the assigned energy values of each node across the path. The node, that acquires less energy, will be included in the route and the node acquiring higher energy consumption is eliminated from the selected path.

VI. RESULTS

Fig. 3: Results

This is first screen when the main.tcl file is executed, it asks for source node and destination node when they both are provided it asks for trust check status. If trust check status is other than "ON" then secured trust aware routing protocol is not activated



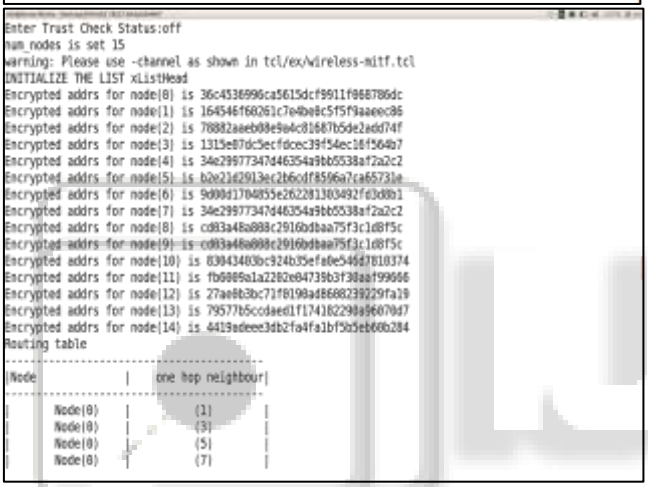


Fig. 4: Results

Then all address of the nodes are encrypted using md5pure algorithm and one hop neighbor of every node are displayed.

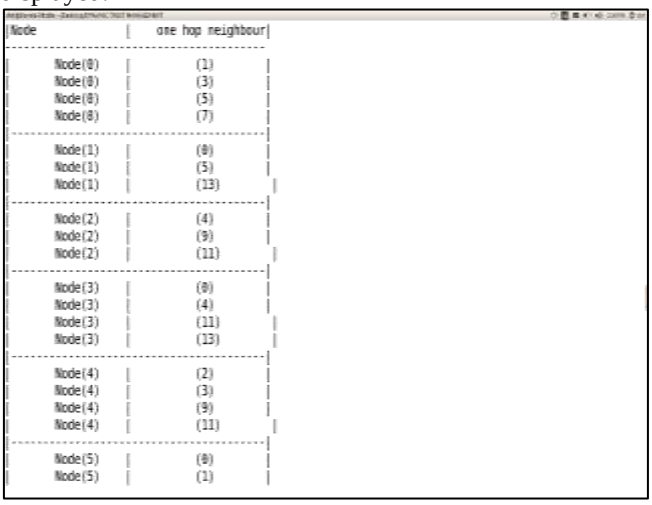


Fig. 5: Results

One hop neighbor of every node are displayed here. Such as one hop neighbor of node 0 is node 1, node 3, node 5, and node 7 as shown in figure.

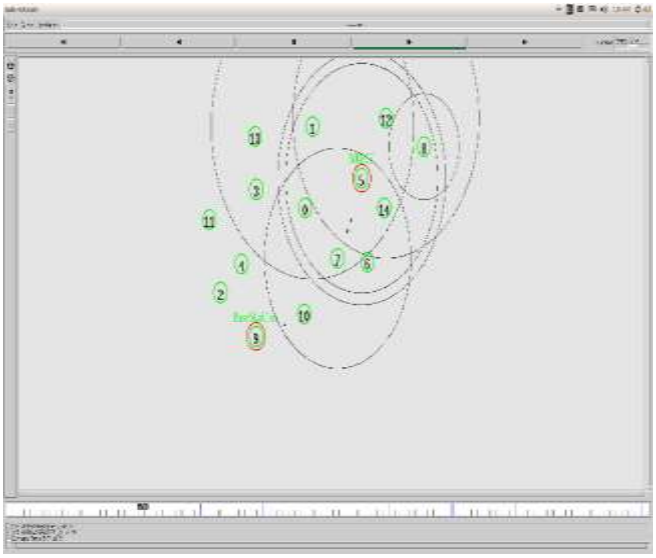


Fig. 6: Results

Node 5 is source and node 9 is destination, node 7 is attacker. But here path selected is 5-7-10-9 which includes the attacker.

Now trust check status is enabled and whole scenario is repeated with same source and destination to check the difference when trust check is enabled and disabled.

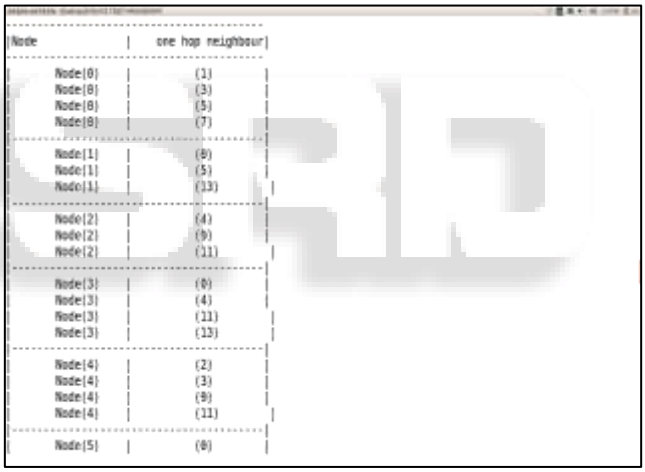


Fig. 7: Results

One hop neighbor of every node are displayed here. Such as one hop neighbor of node 0 is node 1, node 3, node 5, and node 7 as shown in figure.

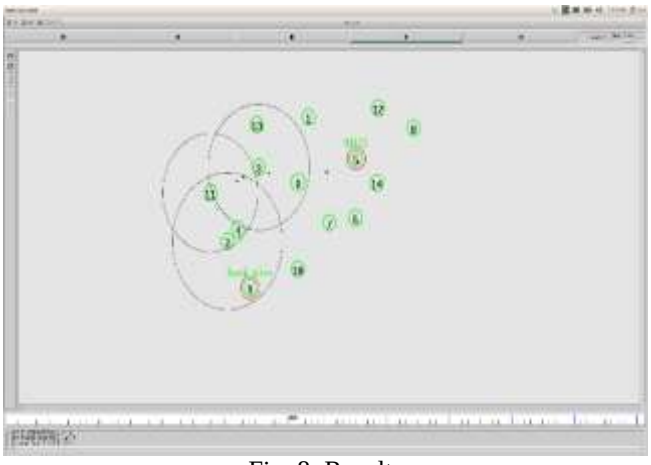


Fig. 8: Results

The previous path 5-7-10-9 is discarded because of node 7 is attacker. So path selected is 5-0-3-4-9 but is the new attacker so this have to be discarded.

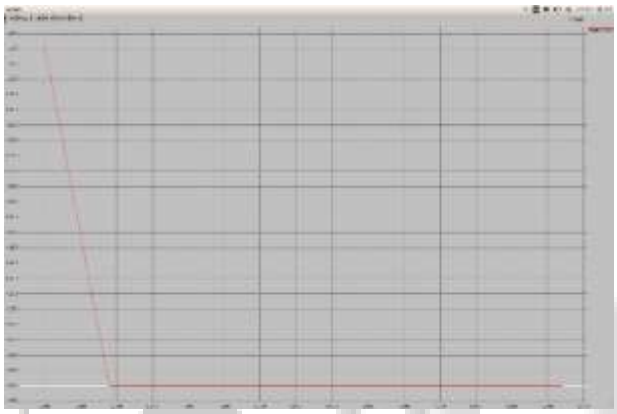


Fig. 9: Xgraph for Packet loss

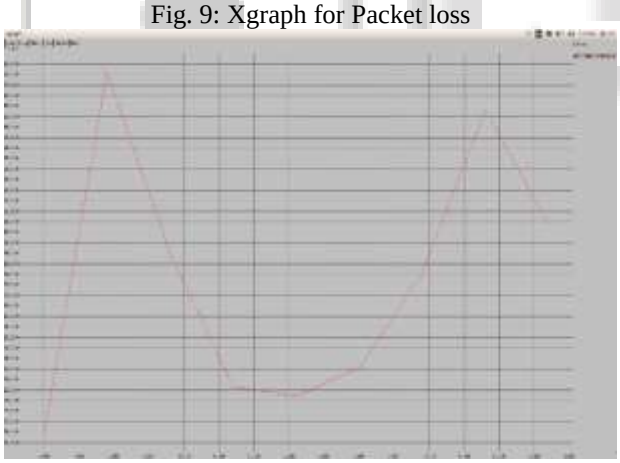


Fig. 10: Xgraph for Packet Delivery Ratio

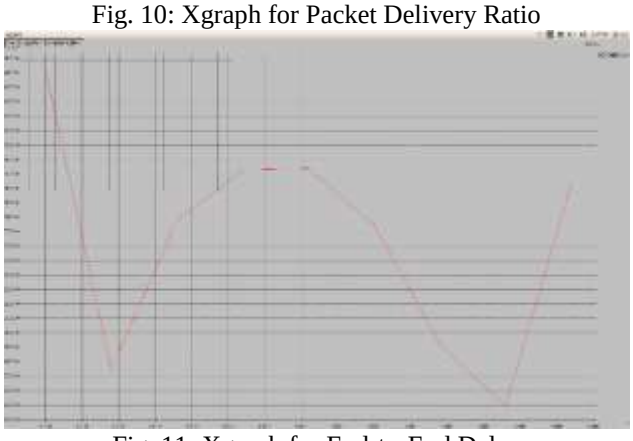


Fig. 11: Xgraph for End-to-End Delay

VII. Conclusion

The proposed work is designed and implemented using secured trust aware routing protocol, an efficient and robust trust aware routing protocol for wireless sensor network, to provide security to multi hop routing in dynamic wireless sensor network against malicious attacks exploiting the retransmission of routing information. Secured trust aware routing protocol, is the proposed routing protocol mainly focuses on trust worthiness of a node and energy efficiency, which are critical issues of wireless sensor network. With the idea of trust management, secured trust aware routing protocol allows a node to know the trust value of its neighbors and thus select a best reliable route for transaction of data.

Unlike existing works on secure routing for wireless sensor networks, secured trust aware routing protocol effectively protects wireless sensor networks from malicious attacks through replaying routing information; it requires neither strict time synchronization nor known geographic information. The resilience and scalability of the specified protocol are proved through both simulation and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, as well as strong attacks such as wormhole attacks and Sybil attacks.

References

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A Trust-Aware Routing Framework for Wireless Sensor Networks," Proc. Seventh European Conf. Wireless Sensor Networks (EWSN '10), 2010.
[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004.
[3] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
[4] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.
[5] M. Jain and H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," Proc. Int'l Conf. Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555-558, 2009.
[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side," Proc. IEEE Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WIMOB '08), pp. 526-531, 2008.
[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Conf. Information Processing in Sensor Networks (IPSN '04), Apr. 2004.

