# AN EFFICIENT TECHNIQUE FOR ROUTING IN WIRELESS SENSOR NETWORK

[1]Akhila, [2]Divyashree B A
[1]M.Tech II year, Department of Computer Science and Engineering, B.N.M Institute of Technology
[2]Professor, Department of Computer Science and Engineering, B.N.M Institute of Technology
Bangalore, India
[1]akhila.arnitha@gmail.com, [2]bnmitcse.divya@gmail.com

***Abstract* -**
**Wireless Sensor Networks have gained popularity due to the fact that they offer low-cost solutions for a variety of application areas, but effective defence against security attacks is a challenging physically insecure environment. Although significant research effort has been spent on the design of trust models to detect malicious nodes based on direct and indirect evidence, this comes at the cost of additional energy consumption. Various secured routing protocols have been developed with the help of cryptographic techniques in order to protect the network against the compromised nodes. However the routing protocols that use encryption schemes require large memory for storing the keys and more computation. The multi hop routing in Wireless Sensor Networks offers little protection against identity deception through replaying routing information. To secure the wireless networks against adversaries misdirecting the multi hop routing, a robust for routing in wireless sensor networks has been developed. The proposed technique uses distance, trust and energy as metrics when choosing the best path towards the destination. A sensor network consists of large number of densely deployed sensor nodes with limited energy and computation. The sensor nodes are susceptible to various types of attacks, since they operate in a**

***Keywords - Wireless Sensor Networks, routing protocol, trust, energy, security***

## I. INTRODUCTION

Wireless sensor network (WSN) [2] consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. to cooperatively pass their data through the network to a main location. A WSN is composed of tens to thousands of sensor nodes, which are low-power, low-cost, small, resource-constrained devices. Using a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path.

WSNs are used in critical applications like military surveillance, homeland security and medical monitoring, and, in these cases, protecting the network against malicious attacks is crucial. However, WSNs have unique characteristics: wireless transmission medium, limited resources available on sensor nodes, hostile environment, adhoc deployment,

unreliable communication, and unattended operation. Therefore, protocols for critical sensor networks should be designed with security in mind, while taking into consideration their specific constraints and challenges. For large sensor networks, multi-hop communication is more energy-efficient than single-hop communication. The multihop routing of wireless sensor networks often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference [3].

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity. The malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic.

It leads to several kinds of attacks like Selective Forwarding, Wormhole, Sinkhole and Sybil attacks [4]. The routing packets, including their original headers, are replayed without any modification. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack. A node in wireless network usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. A fake base station thus could lure more than half the traffic, creating a "black hole." The same technique can be employed to conduct another strong form of attack—Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks.

Most routing protocols for sensor networks use a single metric to determine the best path to destination. Some use two metrics such as location and energy [5], [6], location and trust [7], or trust and link quality [8]. Hence there is a need for a routing framework that can be easily extended to support any metric.

In this paper, we propose a trust and energy-aware, location-based based technique for routing in WSN's. The method uses trust values, energy levels and location information in order to determine the best paths towards a destination. The protocol achieves balancing of traffic load and energy, and generates trustworthy paths when taking into consideration all proposed metrics

## II. RELATED WORK

Based on the network structure, routing in Wireless Sensor Networks can be classified in flat-based, hierarchical based and location-based routing [9]. Based on protocol operation, routing protocols can be classified in multi-path based, query-based, negotiation-based, QoS-based and coherent-based routing protocols.

The relevant routing protocols, which take into consideration trust values when determining the path to the, destination are listed below:

T. Ghosh, N. Pissinou, and K. Makki [10] introduced the Trust-embedded AODV (T-AODV) routing to secure the ad hoc network from independent malicious nodes by finding a secure end-to-end route. When a node wants to find a route to another node, it initiates a route discovery by broadcasting a route request (RREQ) packet. The packet header contains a trust level field, in addition to the other fields in AODV RREQ. When an intermediate node receives the RREQ packet, it rebroadcasts it after modifying the trust level field to include the trust level of the node that sends it the RREQ. Every node checks back the rebroadcasted RREQ packet from its next node to see whether it has provided the proper information. If not, it immediately broadcasts a warning message

questioning the trustworthiness of that node. This protocol does not encourage any intermediate node to send a route reply (RREP). The final route selection is based upon the trust level metric. Hop count plays a role in deciding the final route only when more than one packet has same trust level. The RREP packet has the next hop information. The protocol tries to finds a secure end-to-end path free of malicious nodes and can effectively isolate a malicious entity trying to attack the network independently or in collusion with other malicious entities

A. Rezgui and M. Eltoweissy [11] proposed a routing procedure called Trust Aware Routing Protocol (TARP). It is responsible for routing messages from the different nodes to the base station. TARP is a trust-based routing scheme. Trust refers to the confidence that a node has in a neighbor's cooperation. A node's cooperation, in this context, is the likelihood that it forwards its neighbors' messages. TARP is based on the basic idea of avoiding to route through non cooperative nodes. The intuition is that sending packets to nodes that are not likely to cooperate in routing messages to their neighbors would probably waste energy with no payoff. TARP captures the concept of cooperation in terms of "routing reputation". Informally, reputation is a perception that a node has regarding another node's cooperation. TARP consists of two concurrent phases: (i) reputation assessment and (ii) path reliability evaluation

Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou [12] introduced a routing scheme called Feedback Based Secure Routing protocol (FBSR) for wireless sensor networks. It utilizes feedback information from neighbor nodes to represent the current states of them. On transmission of a packet, the sender prioritizes its neighbors with an evaluation function and places this neighbor list in the packet header. Neighbors, on receiving the packet, will includes its feedback in the ack frame and acknowledges the sender, and in the meantime makes independent decision of whether to forward the packet. FBSR consists of local independent forwarding decisions based on current feedback information and prediction of future conditions. Without any cryptographical protection, the stateless FBSR is resilient to routing state corruption, Wormhole and HELLO flood attacks. To protect FBSR from routing attacks such as Sinkholes and Sybil attacks, we propose the Keyed One Way Hash Chain (Keyed-OWHC) to authenticate the feedback from neighboring nodes.

T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson [13] proposed a location-based trust-aware routing solution called Ambient Trust Sensor Routing (ATSR). It incorporates a distributed trust model which relies on both direct and indirect trust information to protect the WSN from a wide set of routing and trust-related attacks. The routing and trust overhead introduced by ATSR includes the Beacon (broadcast) message which is used by each node to periodically announce its location coordinates, node id and remaining energy, the reputation request (multicast) message used to periodically request indirect trust information and the reputation response (unicast) message which is used to provide indirect information as a reply to a reputation request message.

Most existing routing protocols for WSNs either assume the honesty of nodes or focus on energy efficiency [14], or attempt to exclude unauthorized participation by encrypting data and authenticating packets. Below are some of the examples of these encryption and authentication schemes for WSNs:

A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar [15] proposed SPINS: Security Protocols for Sensor Networks. SPINS includes two building blocks: SNEP and µ*TESLA*. SNEP provides data confidentiality, two-party data authentication, and data freshness for peer-to-peer communication (node to base station). µ*TESLA* provides authenticated broadcast. Each node shares a secret key only with the Base Station and not with any other nodes. Furthermore, the routing tables are calculated by the sink and disseminated to the sensors. The protocol constructs two alternative disjoint paths between each sensor node and the sink. Each message sent from a source to a destination is sent multiple times through each alternative path. The one-way hash chain proposed in µTesla is used to authenticate messages sent by the BS and appropriate MAC mechanisms are implemented to verify the integrity of the packets.

C. Karlof, N. Sastry, and D. Wagner [16] proposed TinySec the first fully-implemented link layer architecture for Wireless Sensor Networks. TinySec supports two different

security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode, TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.

R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus [17] proposed Tinypk: Securing Sensor Networks with Public Key Technology. This security scheme is a mechanism for providing authentication and key exchange between an external party and a sensor network. TinyPK is based on the well-known RSA cryptosystem. All that is required to perform a TinyPK 1024-bit basic public operation is to cube a 1024-bit number and to take its residue modulo a large prime.

In addition to the cryptographic methods, trust and reputation management has been employed in generic ad hoc networks and WSNs to secure routing protocols. Basically, a system of trust and reputation management assigns each node a trust value according to its past performance in routing. Then such trust values are used to help decide a secure and efficient route. However, the proposed trust and reputation management systems for generic ad hoc networks target only relatively powerful hardware platforms such as laptops and smartphones [18], [19], [20], [21].

The proposed protocol is a location-based routing protocol, because it uses the location of neighbor nodes for determining the best path towards the destination. However, it also considers trust and energy when determining the best next hop. In addition, the protocol uses trust values to determine whether to forward packets from specific nodes.

## III. DESIGN

The Trust and Energy-aware Framework Routing is a trust and energy-aware, location-based routing protocol for Wireless Sensor Networks. It includes two phases: setup and forwarding. In the first phase, the best next hop towards the base station is selected by taking into consideration several factors, such as trust, energy and location. In the second phase, the packets generated by trustworthy nodes are forwarded using the selected next hop.

By evaluating trust value of neighboring nodes, the method secures the multi-hop routing in WSNs against attacker misdirecting the routing path. It determines such an attacker by their low trust values. There are several notations are used, they are

**Neighbor:** For a node N, neighboring node of N is reachable from N with one hop wireless transmission.

**Distance:** The distance between two nodes is measured using Euclidean distance formula.

**Trust Rule:** The trust rule defines the trustworthiness of each node based on several criteria such as bandwidth consumption, packet drops etc.

**Energy cost:** For a node N, the energy cost of a neighbor is the average energy cost for successfully deliver a unit sized data packet from current node to next hop node.

The technique secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. The Trust Manager identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. It integrates location, trustworthiness and available energy in making routing decisions. For a node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. To choose its next-hop node, N considers both the trustworthiness and energy of its neighbors. For that, N maintains a neighborhood table with trust level values and energy levels for certain known neighbors.

The Energy Watcher is responsible for recording the Energy Cost for each known neighbor based on node N's observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors. A compromised node may falsely report an extremely low energy cost to lure its neighbors into selecting this compromised node as their next-hop node which is tracked by Trust

Manager. Trust Manager is responsible for tracking trust level values of neighbors based broadcast messages from the base station about data delivery. Once N is able to decide its next hop neighbor according to its neighborhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station.

Consider the Figure 1 in which node A, B, C and D are all honest nodes and not compromised. Node A has node B as its current next-hop node while node B has an attacker node as its next-hop node.

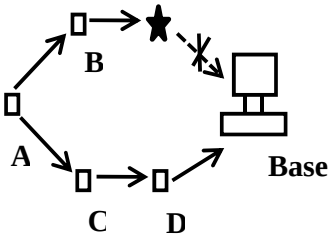


**Figure 1: Working of Trust**

*A. Routing Procedures*

In WSNs, the source node will send detected event of interest to base station through some intermediate nodes. This is the function of multihop routing. In order to maintain stability in routing path, the node will maintain same next hop until next new broadcast message from the base station is occurred. At the same time to reduce the traffic in network, their energy cost reports of that next hop node do not occur until broadcast from base station is changed. If a node does not choose next hop node until next new broadcast message from base station, it will provide guarantee for all path as a loop free path. A node will change their next hop node when their chosen next hop node will receive and deliver data properly.

The attacker drops every packet receives and thus any data packet passing node A will not arrive at the base station. After a while, node A discovers that the data packets it forwarded did not get delivered. The Trust Manager on node A starts to degrade the trust level of its current next-hop node B although node B is absolutely honest. Once that trust level becomes too low, node A decides to select node C as its new next-hop node. In this way node A identifies a better and successful route (A – C – D – Base Station).

*B. Selection of Routing Path*

Each node in WSNs will select the next hop node based on their neighborhood table by considering energy cost and trust value of that node. The node will eliminate attacker node that misdirect traffic by replaying routing information. For node N in WSNs will select the route for sending data to destination such as base station with optimal next hop node from that neighboring node by considering trust level and energy cost and finally forwarded the data to chosen next hop node immediately. Among the remaining neighboring nodes will select next hop node through by evaluating their energy consumption and reliability for successful delivery of packets. Therefore a node will select next hop node with high trust values, it‘s automatically protects the network from an attacker who forges the identity of an attractive node such as base station. The energy driven route is achieved when each node in WSNs will choose their neighbors in terms of energy.

*C. Trust Manager*

Trust, or the trust on the behaviour of the elements of the network, is a key aspect for WSN. A trust management system can be useful for detecting a node which is not behaving as expected (either faulty or maliciously) or it can assist in the decision-making process, for instance, if a node needs a partner in order to achieve a common goal.

Each node in WSNs will select the next hop node based on their neighborhood table by considering energy cost and trust value of that node. The node will eliminate attacker node that misdirect traffic by replaying routing information. For node N in WSNs will select the route for sending data to destination such as base station with optimal next hop node from that neighboring node by considering trust level and energy cost and finally forwarded the data to chosen next hop node immediately. Among the remaining neighboring nodes will select next hop node through by evaluating their energy consumption and reliability for successful delivery of packets. Therefore a node will select next hop node with high trust values, it‘s automatically protects the network from an attacker who forges the identity of an attractive node such as base station. The energy driven route is achieved when each node in WSNs will choose their neighbors in terms of energy. Here

the threshold of battery power is set to 50. A node that has lost its energy below the threshold is not included in transmission.

The Trust Manager keeps track of the trust levels of every node in the network. Suppose if a node tries to enter into the network through identity deception and performs illegal activities that either halt the transmission process or misdirect the data transmission are immediately identified and are reflected in the trust table. However, once the malicious node has been identified the transmission is not stopped but an alternative minimum hop path is taken for routing purpose.

*D. Energy Watcher*

When sensor nodes forwards messages in the network they use their energy in forwarding mechanism but at some point when node depletes it's all energy it fails to transmit further messages resulting in loss of data. Usually, the closest neighbor node will be heavily utilized in routing and forwarding messages while the other nodes are less utilized. This uneven load distribution results in heavily loaded nodes to discharge faster when compared to others. This causes the failure of few over-utilized nodes which results in loss of data, resulting in increase of failed messages in the network. The Energy Watcher takes care of this to minimize the data loss and maximize the lifetime of the network.

The Energy Watcher works on forwarding rule based on location and energy levels of nodes. Each node knows its own geographic location and its own energy levels as well as the location and energy level of its neighbors. The transmitting node writes the geographic position of destination into the packet header and forwards it to the neighbor which is alive (having energy level above than the set threshold) and has the minimum distance among those neighbors having the maximum energy level. In this regime, packet transmission will go on and each node chooses its next hop by following the specified routing technique. This procedure repeats until the packet reaches the destination node.

Packet can terminate in two ways (i.e. successful termination and unsuccessful termination). In successful termination, packets reach to the destination node. While in unsuccessful termination, there are two possibilities. Either destination node is dead or the packet reaches to a node which has no neighbor alive to forward the packet so in this case the packet will drop.

A simple energy model has been used in which every node starts with the same initial energy and forwards a packet by consuming one unit of energy. Initially, all nodes have energy level equal to 100 joules. Each node depletes energy in transmitting and receiving one packet which is equal to 0.1 joule.

## IV. SIMULATION

The nodes are randomly placed in a 600 x 600 $m^2$ field area. The sensor nodes are immobile, so every sensor node is static. Initially, each node has same energy level as specified in energy model. Any node having energy less than or equal to set threshold will be considered as dead. The battery of each node is consumed at the time of sending and receiving packets and at the time of idle state, and it is impossible to communicate when the battery is empty. Total simulation time is 100 seconds. The different simulation parameters that are set are described in the below Table 1.

| **Simulation** | **Values** |
|---|---|
| Simulator | NS 2.34 |
| Geographical area | 600 x 600 |
| Number of nodes | 30 |
| **Channel type** | **Wireless Channel** |
| Radio-propagation | Two Ray Ground |
| MAC type | 802.11 |
| Queue type | DropTail/PriQueue |
| Link layer type | LL |
| Antenna type | Omni Antenna |
| Simulation time (s) | 100 |

**Table 1: Simulation Parameters**

The following are some of the performance metrics evaluated to analyze the simulation results:

Packet Delivery Ratio (PDR) is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

PDR= (S1/S2)* 100

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source. The graph shows the fraction of data packets that are successfully delivered during simulation time

versus the number of nodes. The Snapshot 8.10 highlights the relative performance of existing method without Trust and Energy metrics and with Trust and Energy metrics for Packet Delivery Ratio with varying numbers of nodes of 10,15,20 etc. It is observed that implemented method has a higher Packet Delivery Ratio compared to the existing method.

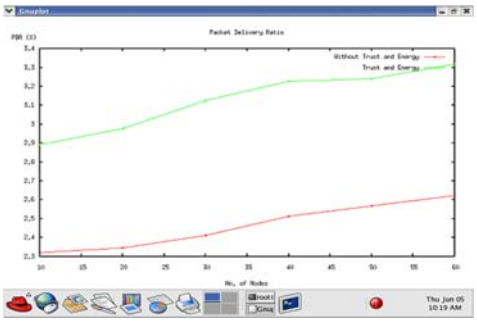

**Figure 2: Packet Delivery Ratio**

End to end delay is defined as the average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as:

Avg. End to end delay= (S/N)

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the destination nodes. The Snapshot 8.11 highlights the relative performance of existing method without Trust and Energy metrics and with Trust and Energy metrics Average End To End delay with varying numbers of nodes of 10,15,20,25 etc. It is observed that implemented method has a lower End to End Delay compared to the existing method.

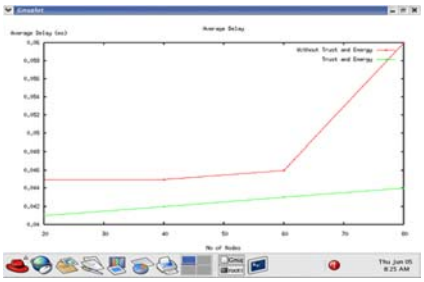

**Figure 3: End to End Delay**

## V. CONCLUSION AND FUTURE WORK

Wireless Sensor Networks that are used for deploying critical applications such as military surveillance or medical monitoring requires the need to provide a high level of security and trustworthiness. Therefore, routing protocols for WSNs should be designed with security in mind, taking into account multiple metrics that support network availability.

The Trust and Energy-aware framework for Routing is a location-based, trust and energy-aware routing mechanism for wireless sensor networks. It uses several metrics: trust values, energy levels, the distance between the local and the neighbor node, and the distance between the neighbor node and the destination. The neighbor with the lowest cost is chosen as next hop towards the base station. The Trust and Energy-aware framework for Routing has two phases: the Setup and the Forwarding phase. In the Setup phase, the next hop is determined, and in the Forwarding phase, the packets generated by trustworthy nodes are forwarded using the selected next hop. It achieves a good balancing of load and energy, and generates trustworthy paths. The implemented technique achieves a higher packet delivery ratio and lower end to end delay.

The future work can address the fact that when the number of isolated malicious nodes increases, some nodes may find them totally surrounded by malicious neighbors and cannot participate effectively in the network. Several mechanisms may be used to solve this issue. One possible solution can be making the nodes that are totally surrounded by malicious neighbors adjust dynamically their belief and disbelief thresholds. Another solution is to give malicious nodes a chance to repent, by letting them broadcast repent packet to their 1-hop neighbors, which can place them on a probation period before deciding whether to forgive them or not.

## VI. REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'12)*, 2012.

[2] F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing*

*Approach*. Morgan Kaufmann Publishers, 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," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed Energy Conservation for Ad Hoc Routing," in ACM/IEEE International Conference on Mobile Computing and Networking,2001,pp.70-84.

[6] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," 2001.

[7] A. Rezgui and M. Eltoweissy, "_RACER: A Reliable Adaptive Service-Driven Efficient Routing Protocol Suite for Sensor-Actuator Networks," IEEE Transactions on Parallel and Distributed Systems, 2009, vol. 20, no. 5, pp. 607-622.

[8] T. Zahariadis, P. Trakadas, H. Leligou, P. Karkazis, and S. Voliotis, "Implementing a Trust-Aware Routing Protocol in Wireless Sensor Nodes," Developments in E-systems Engineering, 2010, pp. 47-52.

[9] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE wireless communications, 2004, pp. 1-37.

[10] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in *Proceedings of Aerospace Conference*, 2004.

[11] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007)*, 8-11 2007.

[12] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "Fbsr: feedback based secure routing protocol for wireless sensor networks," *International Journal of Pervasive Computing and Communications*, 2008.

[13] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson, "Design and implementation of a trust-aware routing protocol for large wsns," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 2, no. 3, Jul. 2010.

[14] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[15] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks Journal (WINET)*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[16] C. Karlof, N. Sastry, and D.Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proc. of ACM SenSys 2004*, Nov. 2004.

[17] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus,"Tinypk: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*. New York, NY, USA: ACM, 2004, pp. 59–64.

[18] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks,"*Wirel. Netw.*, vol. 16, no. 4, pp. 969–984, 2010.

[19] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, "Trust based routing for misbehavior detection in ad hoc networks," *Journal of Networks*, vol. 5, no. 5, May 2010.

[20] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceeding of the 7th Nordic Workshop on Secure IT Systems*, 2003.

[21] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in *Proceedings of Aerospace Conference*, 2004.