# Design and Implementation of Tarf for WSNs

**Kavita, Amareshwari Patil**

M. Tech Student Computer science Department, PDA Eng College, Gulbarga PDA Eng College, Gulbarga

Professor, Computer science Dept, Karnataka, India 585102 Karnataka, India 585102

**Abstract:** ***A wireless sensor network is a collection of nodes organized into a cooperative network. Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. Multi-hop routing in wireless sensor networks (WSNs) offers little protection against deception through replaying routing information. This defect can be taken advantage of by an adversary to misdirect significant network traffic, resulting in disastrous consequences. It cannot be solved solely by encryption or authentication techniques. To secure multi-hop routing in WSNs against intruders exploiting the replay of routing information, we propose TARF, a trust aware routing framework for WSNs.***

**Keywords:** Wireless sensor network, Multi-hop routing, Encryption, Energy efficient

## 1. Introduction

T A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

Wireless sensor networks (WSNs) are ideal candidates for applications such as military surveillance and forest fire monitoring to report detected events of interest. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path. However, the multi-hop routing of WSNs often becomes the target of malicious attacks. In such an attack, the 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.

The paper is organized as follows .Section II introduces related works in this area; Section III presents the proposed solution .Some simulation results are presented in Section IV .Section V concludes the work.

## 2. Related Work

Many of the Target tracking techniques have been implemented in the field of mobile sensor network .However, the design of more efficient target tracking techniques with efficient tracking performance still remain a challenge survey on sensor networks Introduces to recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances.**(F. Akyildiz, W. Su,Y. Sankarasubramaniam, and E. Cayirci[7],** h.).

Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. They proposed security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. They described crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.( **Chris Karlof , David Wagner**).

Wireless communication faces several security risks. An attacker can easily inject bogus packets, impersonating another sender. They referred to this attack as a spoofing attack. An attacker can also easily eavesdrop on communication record packets, and replay the (potentially altered) packets. Here they are concerned of a particularly severe security attack that affects the ad hoc networks routing protocols, it is called the wormhole attack. We can think of wormhole attack as a two phase process launched by one or several malicious nodes. In the first phase, these malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways.( **M. Jain and H. Kandwal**).

Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. Here they systematically analyzed the threat posed by the Sybil attack to wireless sensor networks. They demonstrated that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. and established a classification of different types of the Sybil attack, which enables to better understand the threats posed by each type, and better design countermeasures against each type. They proposed several novel techniques to defend against the Sybil attack, and analyze their effectiveness quantitatively. **(James News ome, Elaine Shi, Dawn Son g, Adri an Perrig).**

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station.( **I. Kron tiris, T. Giannets os, and T. Dimitriou**).

A wireless sensor network (WSN) consisting of a large number of tiny sensors can be an effective tool for gathering data in diverse kinds of environments. The data collected by each sensor is communicated to the base station, which forwards the data to the end user. Clustering is introduced to WSNs because it has proven to be an effective approach to provide better data aggregation and scalability for large WSNs. Clustering also conserves the limited energy resources of the sensors.( **A. Abbasi and M. Younis**).

## 3. Proposed Solution

When the file is sent from the base station in that situation hackers aggravated network conditions. A traditional cryptographic techniques effort does not address the severe problems. That time the file could be affected by hackers. So, the network will be damaged. 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.

Unfortunately, most existing routing protocols for WSNs either focus on energy efficiency assuming that each node is honest with its identity, or they try to exclude unauthorized participation by encrypting data and authenticating packets. Examples of these encryption and authentication schemes for WSNs include TinySec , Spins , TinyPK , and TinyECC. Admittedly, it is important to consider efficient energy usage for battery-powered sensor nodes and the robustness of routing under topological changes and common faults in a wild environment. However, it is also significant to incorporate security as one of the most important goals; meanwhile, even with perfect encryption and authentication, by replaying routing information, a malicious node can still participate in the network using another valid node's identity.

The proposed system focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception the adversary is capable of launching harmful and hard to detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks, and Sybil attacks.

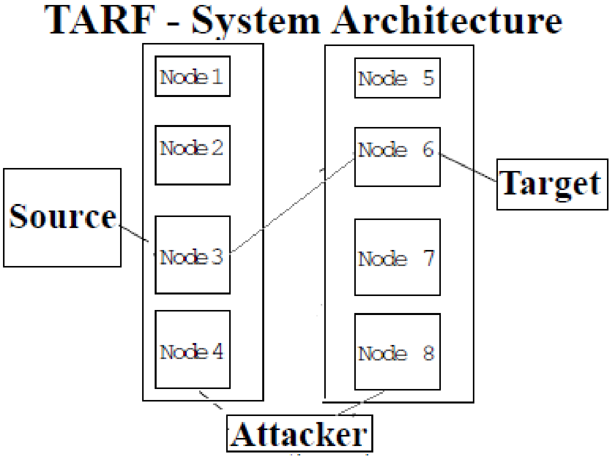
**Advantages of the Proposed System**

- TARF proves effective against those harmful attacks developed out of identity deception.
- TARF gives High Throughput; Throughput is defined as the ratio of the number of all data packets delivered to the base station to destination station.
- Energy is saved in TARF, since it is selecting the next hop based on Trust and Energy Level.
- While selecting the next hop TARF consider energy level and pick the node with high energy level, so that network or single senor node will not come down quickly.
- TARF mainly guards a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft through replaying the routing information.

TARF aims to achieve the following desirable properties:

- ***High Throughput*** - Throughput is defined as the ratio of the number of all data packets delivered to the base station to the number of all sampled data packets. In our evaluation, throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that single-hop retransmission may happen, and that duplicate packets are considered as one packet as far as throughput is concerned. Throughput reflects how efficiently the network is collecting and delivering data. Here we regard high throughput as one of our most important goals.
- ***Energy Efficiency*** - Data transmission accounts for a major portion of the energy consumption. We evaluate energy efficiency by the average energy cost to successfully deliver a unit-sized data packet from a source node to the base station. Note that link-level re-transmission should be given enough attention when considering energy cost since each re-transmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the same energy to transmit a unit-sized data packet, we can use another metric hop-per-delivery to evaluate energy efficiency. Under that assumption, the energy consumption depends on the number of hops, i.e. the number of one-hop transmissions occurring. To evaluate how efficiently energy is used, we can measure the average hops that each delivery of a data packet takes, abbreviated as hop-per-delivery.

- ***Scalability & Adaptability*** - TARF should work well with WSNs of large magnitude under highly dynamic contexts. We will evaluate the scalability and adaptability of TARF through experiments with large-scale WSNs and under mobile and hash network conditions. Here we do not include other aspects such as latency, load balance, or fairness. Low latency, balanced network load, and good fairness requirements can be enforced in specific routing protocols incorporating TARF.



## 4. Formulas for selecting the next node from each level to send the data from source to Destination

### 1. To calculate the trust percentage of each Node:

For all **Nodes in Level1** do:
**Trust_Percentage** = Ack_received / Total_packet_sent

Forall**Nodes in Level2** do:
**Trust_Percentage** = Ack_received / Total_packet_sent

### 2. To calculate Energy Percantage of each node:

Forall**Nodes in Level1** do:
**Energy_Percentage** = 100 - Energy_Cost

Forall**Nodes in Level2** do:
**Energy_Percentage** = 100 - Energy_Cost

### 3. To calculate Node Weight of each Node:

Forall**Nodes in Level1** do:
**Node_Weight** = Trust_Percentage + Energy_Percentage

Forall**Nodes in Level2** do
**Node_Weight** = Trust_Percentage + Energy_Percentage

### 4. Select the Node to transfer the data:

Level1_Node = (Greatest_Node_Weight(Fromall **Nodes in Level1**) ) && (Status = Active)

Level2_Node = (Greatest_Node_Weight(Fromall **Nodes in Level2**) ) && (Status = Active)

**Algorithm for TARP:**
**Step 1**. Get all nodes in the Network.
**Step 2.**Group them into layers.
**Step 3**. Calculate the Node Weight of each node in all the Layers using formula.
For all **Nodes** in **Level1** do **Node Weight = Trust Percentage + Energy Percentage.**
Forall**Nodes** in **Level2** do
**Node_Weight = Trust_Percentage + Energy_Percentage.**
**Step 3**. Select one node from each as “next hop”.
**Level1_Node = (Greatest_Node_Weight(Fromall Nodes in Level1) ) && (Status = Active)**
**Level2_Node = (Greatest_Node_Weight(Fromall Nodes in Level2) ) && (Status = Active)**
**Step 4**. Send the data from Source to Destination through Level1_Node and Level2_Node.

**Snapshots**

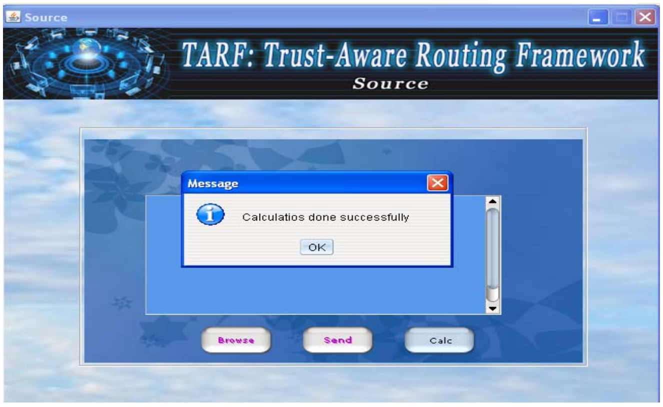

Source
TARF: Trust-Aware Routing Framework
Source
Message
Calculatios done successfully
OK

**Figure :** source node. When we click calc button trust and energy percent of all the nodes of level1 router will be calculated in the database.

## Conclusion

We have designed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information.TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route.

Our main contributions are listed as follows. (1) Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.

Researcher’sfuture work is to further evaluate TARF withlarge-scale WSNs deployed in wild environments and to study how to choose parameters involved for specific applications. They believe that the idea of TARF can also be applied to general ad hoc networks and peer-to-peer networks to fight against similar attacks.

## References

[1] G. Zhan, W. Shi, and J. Deng, “Tarf: A trust-aware routingframework for wireless sensor networks,” in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN’10)*, 2010.

[2] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in *Proceedings of the1st IEEE International Workshop on Sensor Network Protocols andApplications*, 2003.

[3] M. Jain and H. Kandwal, “A survey on complex wormhole attack in wireless ad hoc networks,” in

*Proceedings of International Conference on Advances in Computing, Control, and TelecommunicationTechnologies (ACT '09)*, 28-29 2009, pp. 555 –558.

[4] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *Proceedings of IEEE International Conference on Wireless and MobileComputing, Networking and Communications(WIMOB '08)*, 12-14-2008, pp. 526 – 531.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks:Analysis and defenses," in *Proc. of the 3rdInternational Conference on Information Processing in Sensor Networks(IPSN'04)*, Apr. 2004.

[6] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in *Proceedings of the 10th International Conference on Advanced CommunicationTechnology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[8] A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput.Commun.*, vol. 30, pp. 2826– 2841, October 2007.

[9] C. Intanagonwiwat, R. Govindan, D. Estrin, Directeddiffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of the ACM Mobi-Com'00, Boston, MA, 2000, pp. 56–67.

[10] C. Perkins, Ad Hoc Networks, Addison-Wesley, Reading, MA, 2000.

[11] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Nextcentury challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washingtion, USA, 1999, pp. 263–270.

[12] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, Scalablecoordination for wireless sensor networks: self-configuring localization systems, International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK, July 2001.

[13] Al-Karaki, J., Kamal, A.: Routing techniques in wireless sensor networks: a survey. IEEEWireless Communications 11(6), 6–28 (2004).

[14] Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proceedings of 1996 IEEE Symposium on Security and Privacy, pp. 164–173 (1996)

[15] Boukerche, A., El-Khatib, K., Xu, L., Korba, L.: A novel solution for achieving anonymity in wireless ad hoc networks. In: Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pp. 30–38 (2004)

[16] Ganeriwal, S., Balzano, L., Srivastava, M.: Reputation-based framework for high integritysensor networks. ACM Trans. Sen. Netw. (2008)

[17] He, Q., Wu, D., Khosla, P.: Sori: A secure and objective reputation-based incentive scheme for ad hoc networks. In: Proceedings of IEEE Wireless Communications and Networking Conference, pp. 825–830 (2004)

[18] Kamvar, S., Schlosser, M., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: Proceedings of the 12th international conference on World Wide Web, pp. 640–651 (2003)

[19] Liang, Z., Shi, W.: Pet: A personalized trust model with reputation and risk evaluation forp2p resource sharing. In: HICSS 2005: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS 2005) - Track 7. IEEE Computer Society, Los Alamitos (2005)

[20] Zhan, G., Shi, W., Deng, J.: Poster abstract: Sensortrust a resilient trust model for wsns. In: SenSys 2009: Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (2009)