Implementation Of An Energy Efficient Routing Protocol: Tarf (Trust-Aware Routing Framework)

M. Mohan
Asst.Professor(CSE),SRM University, NCR Campus

Surbhi Tayal
SRM University, NCR Campus

Shalini Tiwari
SRM University, NCR Campus

Abstract

This paper surveys the design and implantation of TARF, a trust aware routing protocol, which works efficiently and securely over wireless sensor networks. This framework has been proposed to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. This defect can be taken advantage of by an adversary to misdirect significant network traffic, resulting in disastrous consequences. Not only does TARF significantly reduce negative impacts from these attackers, but it is also energy-efficient with acceptable control traffic overhead. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying.

1. Introduction

A sensor network is composed of a large number of battery-powered sensor nodes densely deployed over a certain geographical area. These sensor nodes are capable of computing partial data and forwarding it to the base station or a sink node for further processing via a multi-hop path. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. Here, we focus on the kind of attacks developed out of identity deception in which adversaries misdirect the network traffic.

1.1 Blackhole attack

In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages received, just as a black hole absorbing everything passing by. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it, is dramatically decreased. Different locations of the attacker induce different influences on the network. If the attacker is located close to the base station, all the traffic going to the base station might need to go through the attacker. Obviously, black hole attacks in this case can break the communication between the base station and the rest of the WSN, and effectively prevent the WSN from serving its purposes.

1.2 Sinkhole attack

Given certain knowledge of the routing protocol in use, the attacker tries to attract the traffic from a particular region through it. For example, the attacker can announce a false optimal path by advertising attractive power, bandwidth, or high quality routes to a particular region. Other nodes will then consider the path through this attacker node better than the currently used one, and move their traffic onto it. Since affected nodes depend on the attacker for their communication, the sinkhole attack can make other attacks efficient by positioning the attacker in busy information traffic.

1.3 Selective forwarding

Selective forwarding attacks include two cases. In one case (Message Selective Forwarding), the attacker selectively sends the information of a particular sensor; in the other case (Sensor Selective Forwarding), the attacker sends/discards the information from selected sensors. The former attack is considered as the application layer attack while the latter attack is considered as in the network layer and is the focus of our discussion. Obviously, this attack can take place only when the attacker is on the route of packet transfer in a multi-hop network. If the

attacker happens to be on the route, it can just discard the packets from some selected nodes at its will. Otherwise, before the attack can be launched, it needs to position himself in the routing path using other attacks such as the Sybil attack, sinkhole attack and routing table poisoning attack.

1.4 Wormhole attack

A wormhole attack requires two or more adversaries. These adversaries have better communication resources (e.g. power, bandwidth) than normal nodes, and can establish better communication channels (called "tunnels") between them. Unlike many other attacks in the network layer, the channels are real. Other sensors probably end up adopting the tunnels into their communication paths, rendering their output under the scrutiny of the adversaries. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

1.5 Sybil attack

In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device. We refer to a malicious device's additional identities as Sybil nodes.

2. Architecture of TARF

We start by introducing TARF which prevents a wireless sensor network from being a victim of any of the attacks mentioned above exploiting the replay of routing information, which is not achieved by previous security protocols**.** To detect the trust-awareness of the whole path which is affected by the routing information replaying attack, the base station broadcasts at the beginning of each frame period missing the packet providing the source node ID and packet sequence number (start-end sequence numbers).

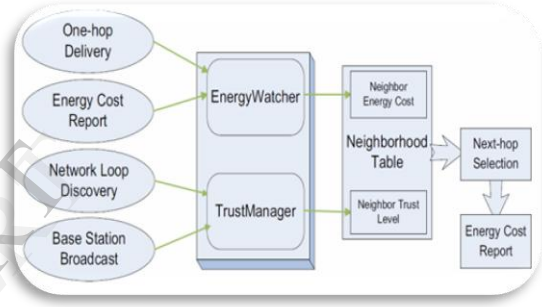


Figure 1 Architecture of TARF

TARF can be developed into a complete and independent routing protocol; the purpose is to allow existing routing protocols to incorporate our implementation of TARF with the least effort and thus producing a secure and efficient fully-functional protocol.

Each node maintains a neighborhood table which consists of Energy report and Trust value of certain known neighbor nodes. Some old entries can be deleted from the table to keep its size acceptable.

Each node N in a WSN consists of two components: Energy watcher and Trust manager.

ENERGY WATCHER: Energy watcher maintains the energy cost report of each neighbor node. This value can be calculated with the help of shortest path algorithm or time taken to deliver data from node to another. For our implementation process, we choose the latter one.

TRUST MANAGER: Trust manager calculates trust value of each neighbor nodes by keeping track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighborhood table.

A very interesting and novel feature is that it proposes that each node calculates the energy cost paid for a unit-packet to reach the base station (i.e. the end-to-end path) taking into account the required retransmissions. A vulnerability introduced here is that for each node to calculate its energy cost, it assumes that its neighbors honestly report their energy costs. $E_{Nb} = E_{unit}/P_{succ} + E_b$

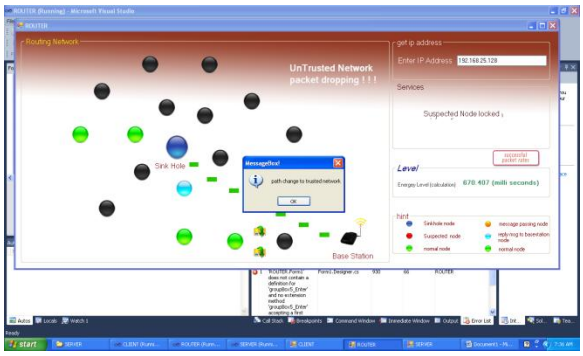
Where E_{Nb} is energy cost of node N transmitting a packet to the sink node through the path passing from neighbor b and P_{succ} is the probability of a transmission being acknowledged, the retransmissions are taken into account. The trust is updated once in each period which is calculated as

$T_{new\_Nb} = (1\text{-}w).T_{old\_Nb} + w.d$

Where T_{old_Nb} is the last calculated trust value, w is the weight assigned to the delivery ratio in the last observation window and d (delivery ratio) is the ratio of successfully delivered to the sink packets over the transmitted packets.

Once E_{Nb} and T_{new_Nb} are calculated successfully, next-hop node is decided and the path is selected which ensures security from different identity deception attacks.

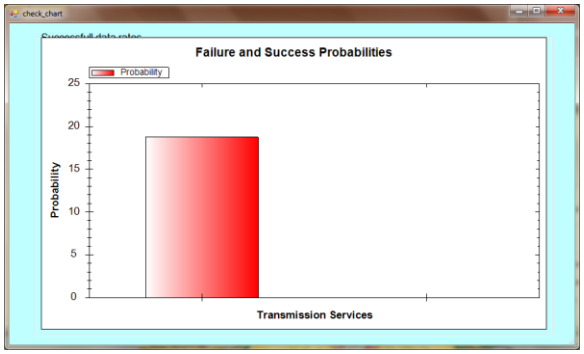
3. Result



In this paper, we presented an overview of design and implementation of 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.

(2) The resilience and scalability of TARF is proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as *wormhole* attacks and *sinkhole attacks*.



The resulting graph shows the transmission probability of the multi-hop path by using TARF. A trusted path is selected which ensures secure transmission of data packet without any identity deception attack. TARF proves efficient against wormhole, Sybil and sinkhole attacks. It neither requires tight time synchronization nor known geographic information.

4. References

1. Lof 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.

2. 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 Telecommunication Technologies (ACT '09)*, 28-29 2009, pp. 555 –558.

3. 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 Mobile Computing, Networking and Communications (WIMOB '08)*, 12-14 2008, pp. 526 –531.

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

5. L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in *Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09)*, 5-7 2009, pp. 378 –383.

6. G. Zhan, W. Shi, and J. Deng, "TARF: A trust-aware routine framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.

7. F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*. Morgan Kaufmann Publishers, 2004.