Trust Aware Routing Framework for WSNs

Vinutha.V & Jayaraj. N
ECE Dept, The Oxford College of Engineering, Bangalore 560060,
E-mail : vinuthav1989@gmail.com, n_jaya_raj@yahoo.com

Abstract – Wireless sensor networks are collection of compact size relatively inexpensive computational nodes that measure local environmental conditions and forward the information to central point for processing. The main task of sensor is to sense and collect data and transmit the information back to specific sites. Wireless sensor networks sends the information from base station through multi-hop path. When information is sent through multiple-hops the protection will be less against the attacks while replaying the routing information. Traditional cryptographic techniques to build the trust aware routing protocol will not consider the severe problems. To safeguard the wireless sensor networks against the oppositions in multi-hop routing TARF (Trust Aware Routing Framework) has been designed and implemented. Without considering the time and other features TARF provides trust worthy and energy efficient route for transmission.

Keywords – Sybil Attack, Sensor Networks, Security

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are large collections of small sensor devices that can be an effective tool for collecting data from various environments. Each sensor sends its data to Base Station (BS), and finally BS sends these data to end user. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. 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. 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.

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. Trust is dependent on time; it can increase or decrease with time based on the available evidence through direct interactions with the same node or recommendations from other trusted nodes. 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. Those 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. WSN 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. 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. an attacker may present multiple identities to the network is known as Sybil attack. A valid node, if compromised, can also launch all these attacks.

II. BLOCK DIAGRAM

![Block Diagram](image)

Fig. 1
Each node selects a next-hop node based on its neighborhood table, and broadcast its energy cost within its neighborhood. To maintain this neighborhood table, Energy-Watcher and Trust Manager on the node keep track of related events to record the energy cost and the trust level values of its neighbors.

### 2.1. Overview

TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy efficient, highly scalable, and well adaptable. Before introducing the detailed design, we first introduce several necessary notions here.

**Neighbor** For a node N, a neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless transmission.

**Trust level** For a node N, the trust level of a neighbor is a decimal number in [0, 1], representing N’s opinion of that neighbor’s level of trustworthiness. Specifically, the trust level of the neighbor is N’s estimation of the probability that this neighbor correctly delivers data received to the base station. That trust level is denoted as T in this paper.

**Energy cost** For a node N, the energy cost of a neighbor is the average energy cost to successfully deliver a unit-sized data packet with this neighbor as its next-hop node, from N to the base station. That energy cost is denoted as E in this paper.

### III. ENERGY WATCHER

A node N’s EnergyWatcher computes the energy cost ENb for its neighbor b in N’s neighborhood table and how N decides its own energy cost EN. Before going further, we will clarify some notations. ENb mentioned is the average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N’s next-hop node being responsible for the remaining route. Here, one-hop re-transmission may occur until the acknowledgement is received or the number of re-transmissions reaches a certain threshold. The cost caused by one-hop re-transmissions should be included when computing ENb. Suppose N decides that A should be its next-hop node after comparing energy cost and trust level. Then N’s energy cost is EN = ENA. Denote EN!b as the average energy cost of successfully delivering a data packet from N to its neighbor b with one hop. Note that the retransmission cost needs to be considered. With the above notations, it is straightforward to establish the following relation:

\[
EN_b = EN!b + Eb
\]  

Since each known neighbor b of N is supposed to broadcast its own energy cost Eb to N, to compute ENb, N still needs to know the value EN!b, i.e., the average energy cost of successfully delivering a data packet from N to its neighbor b with one hop. For that, assuming that the endings of one hop transmissions from N to b are independent with the same probability psucc of being acknowledged, we first compute the average number of one-hop sending is needed before the acknowledgement is received as follows:

\[
\sum_{i=1}^{\infty} psucc \cdot (1 - psucc)^{i-1} = \frac{1}{psucc}
\]  

### IV. TRUST MANAGER

A node N’s TrustManager decides the trust level of each neighbor based on the following events: discovery of network loops, and broadcast from the base station about data delivery. For each neighbor b of N, TNb denotes the trust level of b in N’s neighborhood table. At the beginning, each neighbor is given a neutral trust level 0.5. After any of those events occurs, the relevant neighbors’ trust levels are updated. Note that many existing routing protocols have their own mechanisms to detect routing loops and to react accordingly. In that case, when integrating TARF into those protocols with anti-loop mechanisms, TrustManager may solely depend on the broadcast from the base station to decide the trust level; we adopted such a policy when implementing TARF later. If anti-loop mechanisms are both enforced in the TARF component and the routing protocol that integrates TARF, then the resulting hybrid protocol may overly react towards the discovery of loops. Though sophisticated loop-discovery methods exist in the currently developed protocols, they often rely on the comparison of specific routing cost to reject routes likely leading to loops. To minimize the effort to integrate TARF and the existing protocol and to reduce the overhead, when an existing routing protocol does not provide any antiloop mechanism, we adopt the following mechanism to detect routing loops.

### V. DESIGN OF TARF

For a TARF-enabled 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 considering both the trustworthiness and the energy efficiency. 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. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. It is sometimes necessary to delete some neighbors’ entries to keep the table size acceptable. In TARF, in addition to data packet transmission, there are two types of routing information that need to be exchanged: broadcast messages from the base station about data delivery and energy cost report messages from each node. Neither message needs acknowledgement. A broadcast message from the base station is flooded to the whole network. The freshness of a broadcast message is checked through its field of source sequence number. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbors once. Any node receiving such an energy cost report message will not forward it. For each node N in a WSN, to maintain such a neighborhood table with trust level values and energy cost values for certain known neighbors, two components, Energy-Watcher and Trust-Manager, run on the node Energy-Watcher is responsible for recording the energy cost for each known neighbor, based on 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; however, these TARF-enabled neighbors eventually abandon that compromised next hop node based on its low trustworthiness as tracked by Trust-Manager. Trust-Manager is responsible for tracking trust level values of neighbors based on network loop discovery and 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.

Source will select the next hop node from level 1 nodes. Before selecting, source will check the Node weight of each node. The node which is having more node weight that respective node will be selected as a Next Hop Node. Node weight is the combination of Trust Percentage and Energy Percentage of a respective node. Trust percentage is calculated based on the total files received and for each received file it has to acknowledge to source with success message.

![Fig 2](image-url)  
**Fig 2**: Original topology without malicious node detected

![Fig 3](image-url)  
**Fig 3**: Malicious node has been detected and marked in red

Initial state where intruder will select one node from level1 and level2. For the selected node intruder will keep sending the packets and make the node busy. If any legitimate node send any data to compromised node it will not accept the data in turn it will not give any acknowledgement and gradually trust percentage of this node goes down.

Level 1 will select the next hop node from level 2 nodes. Before selecting Level 1 will check the Node weight of each node. The node which is having more node weight that respective node will be selected as a Next Hop Node from Level 2. Node weight is the combination of Trust Percentage and Energy Percentage of a respective node. Trust percentage is calculated based on the total files received and for each received file it has to acknowledge to Level 1 with success message. Finally Level 2 will forward the data to destination.

VI. REFERENCES


