A Framework for Improving Security Efficiency in Wireless Sensor Networks

[1] **Soumya B,** [2] **Pramela Devi S**

[1] Department of Computer Science & Engineering, MVJ College of Engineering
Bangalore, Karnataka, India

[2] Department of Computer Science & Engineering, MVJ College of Engineering
Bangalore, Karnataka, India

Abstract - Networks are affected by various types of attacks such as sinkhole attacks, wormhole attacks and Sybil attacks. Cryptographic techniques for developing routing protocols do not address these problems. To secure WSNs against multihop routing, a framework is designed for dynamic WSNs. The framework demonstrates steady improvement in network performance by providing trust worthy and energy efficient route. The effectiveness is verified through extensive evaluation with simulation and empirical experiments on large scale WSNs.

Keywords- *WSNs, multih*op routing, security, framework.

1. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

.

A WSN is comprised of sensor nodes which are powered by battery. A sensor node sends messages to the base station within communication range using multihop path. The multihop 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.

The network is subjected to various types of attacks. The harm of malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection and various applications it greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and actual user.WSNs are characterized with denser levels of node deployment, higher unreliability of sensor nodes, severe power and memory constraints. Various design challenges of WSNs are energy efficiency, data delivery models, quality of service, overheads and so on. The current routing protocols either have no security consideration at all, based on the fundamental assumption that the sensor nodes will cooperate and not cheat, or focus on the efficient use of cryptographic mechanisms to authenticate routing packets. In addition, the cryptography based routing mechanisms can only achieve a certain level of security by preventing external attackers. They are ineffective when dealing with compromised, misconfigured or malfunctioning nodes. The reason is that current routing protocols have no notion of trust leading sensor nodes to blindly accept cryptographically authenticated routing information from other nodes. The conventional view of security based on cryptography and authentication alone is not sufficient to provide a complete solution for developing trustworthy sensor networks.

2. Routing Challenges in Sensor Networks

Some of the routing challenges in WSN are as follows

(a).Energy Consumption: As sensor nodes in WSN have limited battery power, it becomes challenging to perform computation and transmission while optimizing energy consumption. In fact the transmission of one bit of data consumes more energy than processing the same bit of data. Sensor node life time strongly depends on its battery life [3].

(b).Node Deployment: Sensor nodes are usually densely deployed in the field of interest depending on application thus influencing the performance of a routing protocol. The deployment can be either deterministic or self-organizing. In deterministic case, the sensor nodes are manually placed and sensed data is routed through determined paths.

(c).Data Delivery Models: Data delivery models can be time driven, data driven, query driven and hybrid (combination of delivery models) depending on the application of sensor nodes and time criticality of data reporting. These data delivery models highly influence the design of routing protocols especially with regard to reducing energy consumption.

(d).Node Capability: Depending on the application, a sensor node can have different role or capability such as relaying, sensing and aggregation since engaging all these functions on the same node would drain the energy of that node more quickly.

(e).Network Dynamics: Most of the network architectures assume that sensor nodes are static but the mobility of base stations and sensor nodes is necessary in some applications. Routing packets in such dynamic architectures becomes challenging in addition to minimizing energy consumption and bandwidth utilization.

3. Problem Statement

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. 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, which is known as a wormhole attack.

A node in a 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. It may drop packets received, forward packets to another node not supposed to be in the routing path, or form a transmission loop through which packets are passed among a few malicious nodes infinitely.
Sinkhole attacks can be launched after stealing a valid identity, in which a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a “black hole.” This 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.

4. Potential Attacks on Existing Routing Protocols

Considering the application and inherent characteristics of WSNs, existing research efforts on routing protocols shift their focus from the traditional address-centric approaches to a more data-centric approach [2]. Directed Diffusion is one representative data-centric routing protocol. After it, many other protocols have been proposed either based on Directed Diffusion or following a similar concept. It has been shown that most of the existing sensor network routing protocols are highly susceptible to attacks. To show how to build the trust into the routing protocol, we take one routing protocol, Gradient Based Routing (GBR) as a representative, and characterize the possible misbehaviors the attackers may conduct. We also discuss some possible handling methods. It should be noted that our proposed trust-aware dynamic routing solution is not limited to any particular routing protocol, and is considered as routing protocol independent, thus it can be easily integrated into existing routing protocols with minor modifications. The GBR is selected just due to its simplicity and popularity. The key idea in GBR is to memorize the number of hops when the interest is diffused through the whole network. As such, each node can calculate a parameter called the height of the node, which is the minimum number of hops to reach the base station. There are two steps in the routing process, interest propagation and path setup.

The potential attacks can occur in both steps. For example, a malicious node may forge bogus interest messages in order to cause high depletion of network energy or collect data for its own interest, and the source authentication could potentially prevent this type of attacks. It may replay messages, but with a high risk of being detected by the reception node using interest caches. It may conduct selective forwarding attack, and get caught easily by a watchdog like misbehavior detection method. It may conduct a blackhole attack by inserting a smaller height for claiming a shorter path to the sink, and afterwards, to enhance its chance to be selected in the routing path. One possible way to deal with this attack is to verify the height information, by checking the consistency of the reported height values from multiple nodes, and trying to figure out any inconsistency caused by the malicious node. This mechanism works well based on the fundamental assumption that there is internal redundancy in the network, while, fortunately it is true for most of the sensor networks. The malicious node may also conduct wormhole attacks by tunneling message received from one part of the network to another through a low-latency out-of-bound link. Under this attack, the network topology gets changed, due to the additional physical capability of the malicious node. The idea of inconsistency checking may help to detect this type of attack.

In order to improve the efficiency, a framework is designed for WSNs.

5. Proposed Method

To protect WSNs from the harmful attacks exploiting the replay of routing information, a robust trust-aware routing framework is designed in order to secure routing solutions in wireless sensor networks. The framework can be developed into a complete and independent routing protocol. The purpose is to allow existing routing protocols to incorporate our implementation of framework with the least effort and thus producing a secure and efficient fully-functional protocol.

5.1 Working of Framework

The neighbor nodes of the source nodes are taken into consideration while creating multipath. 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 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. The framework makes use of trust and energy values to determine the path between source and destination.

(a).Trust Value
That trust level is denoted as T. Trust value is assigned for each and every node, the numeric value such as 0 or 1 is assigned, whereas 0 is considered to be malicious node and trust value 1 is considered to be normal node. Based upon the assigned trust value, the routing path is constructed. The node, which has trust value 1, will be included in the route rather than the node having trust level 0.

(b).Energy Value
Energy cost is denoted as E. Energy value is assigned for each and every node, the numeric value such as 1, 2, 3 is assigned, whereas 1 is considered to be less energy consumption rather than 2 or 3. Based upon the assigned energy, the routing path is constructed. The node, which acquires less energy, will be included in the route rather than the higher energy consumption.

Though a specific application may determine whether data encryption is needed, framework requires that the packets are properly authenticated, especially the broadcast packets from the base station [1]. The broadcast from the base station is asymmetrically authenticated so as to guarantee that an adversary is not able to manipulate or forge a broadcast message from the base station at will. Importantly, with authenticated broadcast, even with the existence of attackers, framework may use trust values and the received broadcast packets about delivery information to choose trustworthy path by circumventing compromised nodes. Without being able to physically capturing the base station, it is generally very difficult for the adversary to manipulate the base station broadcast packets which are asymmetrically authenticated. The asymmetric authentication of those broadcast packets from the base station is crucial to any successful secure routing protocol. It can be achieved through existing asymmetrically authenticated broadcast schemes that may require loose time synchronization.

5.2 Advantages

(a) Based on the unique characteristics of resource-constrained WSNs, the framework centers on trustworthiness and energy efficiency.

(b) Framework requires neither tight time synchronization nor known geographic information.

(c) Framework proves resilient under various attacks exploiting the replay of routing information, which is not achieved by previous security protocols.

(d) Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition, framework demonstrates steady improvement in network performance.

(e) Framework module proves low overhead.

6. Conclusion

A robust trust aware routing framework for WSNs secures multihop routing in dynamic WSNs against harmful attackers by exploiting the replay of routing information. Framework 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, framework enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. This prospective has a noticeable impact on WSN for their strong energy efficiency, robustness and self configuration requirements. Framework effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.

References

[1] Guoxing Zhan, Weisong Shi, “Design and Implementation of TARF: Trust-Aware Routing Framework for WSNs” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, March/April 2012

[2] 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

[3] sRajashekhar C. Biradar “A Survey on Routing Protocols in Wireless Sensor Networks”, 2012.