SMART: Secure Multi-pAths Routing for wireless sensor neTworks

Noureddine Lasla[1], Abdelouahid Derhab[2], Abdelraouf Ouadjaout[1], Miloud Bagaa[1], and Yacine Challal[3]

[1] Department of Theories and Computer Engineering, CERIST, Algiers, Algeria
[2] Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia
[3] Laboratoire de Méthodes de Conception des Systèmes (LMCS), Ecole nationale Supérieure d'Informatique, Algiers, Algeria

Abstract. In this paper, we propose a novel secure routing protocol named Secure Multi-pAths Routing for wireless sensor neTworks (SMART) as well as its underlying key management scheme named *Extended Two-hop Keys Establishment* (ETKE). The proposed framework keeps consistent routing topology by protecting the hop count information from being forged. It also ensures a fast detection of inconsistent routing information without referring to the sink node. We analyze the security of the proposed scheme as well as its resilience probability against the forged hop count attack. We have demonstrated through simulations that SMART outperforms a comparative solution in literature, i.e., SeRINS, in terms of energy consumption.

1 Introduction

Wireless sensor networks (WSNs) [1] are defined as a large collection of tiny sensor nodes, which have scarce resources regarding energy, bandwidth, processing capacity and storage. Such networks are designed to gather data in inhospitable places and might be involved in critical applications meant for civil and military use. The main task of a wireless sensor network is to collect/aggregate data from the sensor nodes and transmit them towards the sink node using a hop-by-hop communication. In these critical applications, establishing a reliable path free of compromised nodes is an important security concern.

The single-path routing is not resilient to attacks as it is sufficient to compromise one node along the path to cause path failure. To deal with this failure, a path maintenance process is initiated to find a new path, which is costly in terms of time, control overhead, and energy consumption. The use of multi-path routing can be a good solution against attacks that target the reliability of the network. As data are transmitted redundantly through multiple paths, the packets are likely to reach the sink even in the presence of some compromised nodes.

The attacks against wireless sensor networks can be either *insider* or *outsider* according to whether or not the adversary retrieves the information stored in

S. Guo et al. (Eds.): ADHOC-NOW 2014, LNCS 8487, pp. 332–345, 2014.

the sensor nodes. Using cryptography mechanism, the outsider attacks can be avoided as there is no way for an attacker to inject or read information from the network. The insider attack, however, is more powerful as by compromising a set of sensor nodes, an adversary can get access to the security materials of these nodes, change their running codes, and inject false information. For example, in routing construction protocols, an adversary can succeed at launching the Sinkhole attack by simply injecting a faked shortest path RREQ message using the cryptographic materials of the compromised nodes.

To construct the routing topology, different metrics are employed. Among them, we can find the hop count, sequence number, path identifier, etc. The hop count for example is used to select the shortest path leading to the sink and avoid routing loops, where each node should increment it by one before relaying it to its next hop. However, these metrics are mutable information, meaning that every node could manipulate it during the relay. In a security context, this mutable information is attractive for adversaries who want to compromise the network and can be exploited by many attacks like the sinkhole and the wormhole attacks. Using only cryptography techniques to ensure the integrity of route construction information (hop count, sequence number, etc.) is not sufficient especially when the adversary compromise a set of nodes in the network, as mentioned earlier. For these reasons, detecting compromised nodes is an important security concern that should be considered when designing a secure communication protocol.

In the literature, some solutions [2–5] have been designed to build a reliable routing topology. Authors in [5] propose a protocol to secure tree construction, based on braodcast key to authenticate neighboring nodes. However, although this protocol is resilient to node replication attack, the protocol cannot protect the transmitted routing information from being altered or forged when an adversary compromise a node. SEIF [3] allows the construction of more alternative disjoint paths belonging to different sub-branches. Each path from different sub-branches can be only intersected at nodes that are at one hop from the sink, and each sub-branch is tagged with a unique identifier that guarantees the construction of such topology. Furthermore, to ensure the security of the sub-branch identifiers, authors use a set of one-way hash chains to authenticate messages from the sink and the sub-branches origin. Therefore, any attempt of injecting faked sub-branch identifier can be immediately detected even if the adversary make an inside attack. However, SEIF cannot detect a Wormhole attack, when an adversary captures a valid hash chain of sub-branches from one end and replay them at the other end [6]. In addition, SEIF does not consider any metric to carry out the routing decision.

SeRINS [2] is a semi-distributed solution based on the hop count metric to select routes. This protocol provides a mechanism to protect the hop count information at the sensor node level with the help of the sink. Each sensor, first, chooses its first parent that will be used as a reference to verify the correctness of any received alternate route. After that, when a node suspects on one alternate route, it sends an alert to the sink, which makes a decision about whether the suspected or the alert sender node is malicious. However, involving the sink in