Secure Routing in Wireless Sensor Networks

Leonardo Leiria Fernandes
leiria@itc.it
Ida Sri Rejeki Siahaan
ida.siahaan@dit.unitn.it

Introduction to Wireless Sensor Networks
Report
University of Trento
June 2007

Supervisor:
Roberto Passarone

1 Introduction

Routing in wireless sensor networks has been reasonably well studied and most current research has focused primarily on providing the most energy efficient routing. However, there is a great need for both secure and energy efficient routing protocols in wireless sensor networks, as demonstrated by sinkhole, wormhole and Sybil attacks [10]. Therefore, routing security must not be an after-thought, but rather it must be included as part of the overall sensor network design, as wireless sensor networks continue to grow in size and utility.

In general, packet routing algorithms are used to exchange messages with sensor nodes that are outside of a particular radio range. This is different to sensors that are within radio range where packets can be transmitted using a single hop. In such single hop networks security is still a concern, but is more accurately addressed through secure broadcasting and multicasting. Furthermore, one hop sensor networks are not recommended in most applications due to the energy cost of long range transmissions.

The routing techniques in wireless sensor networks at the present have the common objective of trying to extend the lifetime of the sensor network while not compromising data delivery. Moreover, the routing techniques are classified based on the network structure as depicted on Fig. 1 into three categories: flat, hierarchical, and location-based routing protocols. Furthermore, these protocols are classified into multipath-based, query-based, negotiation-based, and QoS-based routing techniques depending on protocol operation with design trade-offs between energy and communication overhead savings.

This document presents a survey of the security threats and countermeasures discussed in the literature of the sensor networking area. In the next section a general overview of several routing protocols is presented. Next, we survey some security requirements and threats in sensor networks, as well as the respective countermeasures. Finally we draw some conclusions on the topic.

2 Routing in Wireless Sensor Networks

Sensor networks are different from other communication networks. Usually, there is no sense in establishing a point to point connection between two arbitrary sensor nodes in the network, as is the case in traditional computer networks. Instead, the destination of all data is usually a small set of nodes called base stations or sinks in the sensor networks terminology. Often one single sink is available. In this sense, Sensor networks can be seen as converge-cast networks. In many cases nodes do not even have unique identifications.

Communication is often done through the propagation of an interest from a sink in the network and replies from the nodes that can match such interests back to the sink, as proposed in the directed diffusion protocol [9]. Nodes that provide data to the sinks are usually called data sources, or simply sources. For example, assume humidity sensors are distributed in a field and they have approximate information about their position. An interest from the sink could be a message asking about humidity on a specific area of the field. By knowing their position and the area of interest, sensors can determine if they should become a source and reply to the message or not. If a reply is sent, it could be forwarded to the sink by the reverse path through which the interest has come.

Interests are often flooded in the network. Such flood allows nodes to keep information about which neighbors they should forward application messages to, i.e. the ones they received interest messages from.

To perform this kind of interest propagation and converge-cast in the most energy-efficient way possible is the wireless sensor networks routing problem. Concerns like load balancing and data aggregation are frequent goals of research on the topic.

There is a large number of approaches to the problem in the literature.

LEACH [6] presents an hierarchical solution. In this protocol nodes are divided in clusters. All data from the nodes in the cluster are sent to a special node called "cluster head". The cluster head is responsible for performing the transmission to the sink. The role of cluster head is rotated between nodes for load balancing, which requires the execution of a leader election algorithm in the cluster. This protocol assumes that all nodes are within communication range of each other and of the sink. That is very often not the case in real world sensor networks.

An approach used in TEEN [12] defines thresholds. Only data that varies from the previous sent data by a value greater than the threshold is supposed to be transmitted according to this protocol.

In the work by Beyens et al. [2], a learning algorithm is used to improve routing. Sensors receive reinforcement messages from neighboring nodes when they perform a good behavior, like forwarding a message to a node that can aggregate data from different sources, for example. Reinforced behaviors have their probability of being repeated in the future increased by the algorithm.

Gan, Liu and Jin [3] propose a protocol in which agents are created on data sources to transport the data through the network to the destination. Such agents gather information available at each node before deciding which node to go next.

3 Security in Wireless Sensor Networks

This section describes the security requirements of sensor networks as well as common attacks to this kind of network and the respective countermeasures.

3.1 Security Requirements

The requirements of a wireless sensor network encompass both the typical network requirements and the unique requirements suited solely to wireless sensor networks [14]:

Data Confidentiality In most applications nodes communicate very sensitive data such as surveillance information and industrial secrets. Such applications need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption;

Data Integrity To ensure that information is not changed in transit, either due to malicious intent or by accident;

Data Freshness To ensure the freshness of each message such that the data is recent, and to ensure that no old messages can be replayed;

Availability We can loose the availability of a sensor due to the lost of energy because of computation and communication, while a single point failure will be introduced if using the central point scheme which makes us loose the availability of sensor network;

Self-Organization Distributed sensor networks must self-organize to support multihop routing. Such self organization is very hard to be done in a secure way;

Secure Localization The utility of a sensor network often relies on its ability to accurately and automatically locate each sensor in the network. However, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc;

Authentication Verifying that principals are who they claim to be can be achieved through appropriate proof of identity (i.e. encrypted signature).

3.2 Security Threats to Sensor Networking

Sensor network routing protocols are usually simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. We can categorize the network layer attacks against sensor networks as follows [10]:

Spoofed, altered, or replayed routing information Attacks targeted at the routing information exchanged between nodes so that adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.

Selective forwarding Malicious nodes in multi-hop networks may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.

Sinkhole attacks The adversary collects nearly all the traffic from a particular area through a compromised node, creating a sinkhole with the malicious node at the center.

Sybil attacks A single adversary node presents multiple identities to other nodes in the network [**?**].

Wormholes An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part [8].

`HELLO` **Flood attacks** Many protocols require nodes to broadcast `HELLO` packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor.

Acknowledgement spoofing Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

3.3 Countermeasures

Due to the attacks described in the previous section, security must be taken into account in sensor network routing protocols. However, most proposed sensor network routing protocols, have been designed without security in mind. The first attempt to analyze security goals for routing protocols in sensor networks [10] proposes threat models and shows how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks. Furthermore, in order to fulfill the security goals, we have to consider the characteristic of sensor networks, namely resource-starved nature, very little computational power such that public-key cryptography is so expensive as to be unusable, communication bandwidth is extremely dear so that each bit transmitted consumes about as much power as executing more than 8 million instructions, and power is the scarcest resource of all.

We have the setting of the security model, namely insecure wireless communication, limited node capabilities, possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network. The countermeasures to the attacks as presented in [10]:

3.3.1 Outsider attacks and link layer security

The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. The Sybil attack is no longer relevant because nodes are unwilling to accept even a single identity of the adversary. The majority of selective forwarding and sinkhole attacks are not possible because the adversary is prevented from joining the topology. Link layer acknowledgements can now be authenticated. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks. Although an adversary is prevented from joining the network, nothing prevents her from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part to convince them they are neighbors or by amplifying an overheard broadcast packet with sufficient power to be received by every node in the network.

If a wormhole has been established, encryption may make some selective forwarding attacks against packets using the wormhole more difficult, but clearly can do nothing to prevent "black hole" selective forwarding. Link layer security mechanisms using a globally shared key are completely ineffective in presence of insider attacks or compromised nodes. Insiders can attack the network by spoofing or injecting bogus routing information, creating sinkholes, selectively forwarding packets, using the Sybil attack, and broadcasting HELLO floods.

3.3.2 The Sybil attack

An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even nonexistent) node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. In order to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network, the base station can reasonably limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it. Thus, when a node is compromised, it is restricted to (meaningfully) communicating only with its verified neighbors. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an adversary can still use a wormhole to create an artificial link between two nodes to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

3.3.3 HELLO flood attacks

HELLO flood attacks can be defensed against by verifying the bidirectionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol described in [10] is sufficient to prevent HELLO flood attacks. Not only does it verify the bidirectionality of the link between two nodes, but even if a well-funded adversary had a highly sensitive receiver or had wormholes to a multiple locations in the network, a trusted base station that limits the number of verified neighbors for each node will still prevent HELLO flood attacks on large segments of the network when a small number of nodes have been compromised.

3.3.4 Wormhole and sinkhole attacks

Wormhole and sinkhole attacks are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole. When routes are established simply based on the reception of a packet as in TinyOS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify. A technique for detecting wormhole attacks is presented in [7], but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Because it is extremely difficult to retrofit existing protocols with defenses against these attacks, the best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless. For example, one class of protocols resistant to these attacks is geographic routing protocols. Protocols that construct a topology initiated by a base station are most susceptible to wormhole and sinkhole attacks. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station. Because traffic is naturally routed towards the physical location of a base station, it is difficult to attract it elsewhere to create a sinkhole. A wormhole is most effective when used to create sinkholes or artificial links that attract traffic. Artificial links are easily detected in geographic routing protocols because the *neighboring* nodes will notice the distance between them is well beyond normal radio range.

3.3.5 Leveraging global knowledge

A significant challenge in securing large sensor networks is their inherent self-organizing, decentralized nature. When the network size is limited or the topology is well-structured or controlled, global knowledge can be leveraged in security mechanisms.

Consider a relatively small network of around 100 nodes or less. If it can be assumed that no nodes are compromised during deployment, then after the initial topology is formed, each node could send information such as neighboring nodes and its geographic location (if known) back to a base station. Using this information, the base station(s) can map the topology of the entire network. To account for topology changes due to radio interference or node failure, nodes would periodically update a base station with the appropriate information. Drastic or suspicious changes to the topology might indicate a node compromise, and the appropriate action can be taken. We have discussed why geographic routing can be relatively secure against wormhole, sinkhole, and Sybil attacks, but the main remaining problem is that location information advertised from neighboring nodes must be trusted. A compromised node advertising its location on a line between the targeted node and a base station will guarantee it is the destination for all forwarded packets from that node. Probabilistic selection of a next hop from several acceptable destinations or multipath routing to multiple base stations can help with this problem, but it is not perfect. When a node must route around a *hole*, an adversary can *help* by appearing to be the only reasonable node to forward packets to. Sufficiently restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known. For example, nodes can be arranged in a grid with square, triangular, or hex shaped cells. Every node can easily derive its neighbors' locations from its own, and nodes can be addressed by location rather than by an identifier.

3.3.6 Selective forwarding

A compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a base station.

Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised. However, completely disjoint paths may be difficult to create. Braided paths [15] may have nodes in common, but have no links in common (i.e., no two consecutive nodes in common). The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

3.3.7 Authenticated broadcast and flooding

Since base stations are trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station. This requires some level of asymmetry: since every node in the network can potentially be compromised, no node should be able to spoof messages from a base station, yet every node should be able to verify them. Authenticated broadcast is also useful for localized node interactions. Many protocols require nodes to broadcast `HELLO` messages to their neighbors. These messages should be authenticated and impossible to spoof. Proposals for authenticated broadcast intended for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of typical sensor network packet.

μTESLA [13] is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. μTESLA achieves the asymmetry necessary for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains constructed with a publicly computable cryptographically secure hash function. Replay is prevented because messages authenticated with previously disclosed keys are ignored.

μTESLA also requires loose time synchronization. Flooding [4] can be a robust means for information dissemination in hostile environments because it requires the set of compromised nodes to form a vertex cut on the underlying topology to prevent a message from reaching every node in the network. The downsides of flooding include high messaging and corresponding energy costs, as well as potential losses caused by collisions. SPIN [11] and gossiping algorithms [5] are techniques to reduce the messaging costs and collisions which still achieve robust probabilistic dissemination of messages to every node in the network.

4 Conclusion

Sensor network routing protocols must be designed with security in mind [10]. We have seen that Link-layer encryption and authentication, multipath routing, identity verification, bidirectional link verification, and authenticated broadcast can protect sensor network routing protocols against outsiders, bogus routing information, Sybil attacks, `HELLO` floods, and acknowledgment spoofing, and it is feasible to augment existing protocols with these mechanisms. Sinkhole attacks and wormholes pose significant challenges to secure routing protocol design, and it is unlikely there exists effective countermeasures against these attacks that can be applied after the design of a protocol has completed. It is crucial to design routing protocols in which these attacks are meaningless or ineffective. Geographic routing protocols are one class of protocols that holds promise.

A limitation of building a multi-hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. If a significant number of these nodes have been compromised then all is lost. This indicates that clustering protocols like LEACH where cluster-heads communicate directly with a base station may ultimately yield the most secure solutions against node compromise and insider attacks.

Furthermore, a randomly rotating set of *virtual* base stations for creating an overlay network may be an option. The idea is that after a set of virtual base stations have been selected, a multi-hop topology is constructed using them. The virtual base stations then communicate directly with the real base stations. The set of virtual base stations should be changed frequently enough to make it difficult for adversaries to choose the *right* nodes to compromise.

We believe it is still an open problem to design a sensor network routing protocol that satisfies both the proposed security goals and achieve the power savings of state-of the-art sensor network routing protocols. That is because such protocols often rely on self-organization and on nodes and even the base station having only local information. In such paradigm where the system is not globally known it is very hard to achieve security. To obtain global knowledge is often a task too expensive for sensor networks.

Discuss the state-of-the-art, highlighting the Give directions for future work,

References

[1] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6):6–28, 2004.

[2] Pieter Beyens, Maarten Peeters, Kris Steenhaut, and Ann Nowe. Routing with compression in wireless sensor networks: a q-learning approach. In *Fifth Eu-*

ropean Workshop on Adaptive Agents and Multi-Agent Systems, pages 575–578, Washington, DC, USA, 2005. IEEE Computer Society.

[3] Long Gan, Jiming Liu, and Xiaolong Jin. Agent-based, energy efficient routing in sensor networks. In *AAMAS '04: Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems*, pages 472–479, Washington, DC, USA, 2004. IEEE Computer Society.

[4] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker. An empirical study of epidemic algorithms in large scale multihop wireless networks. Technical report, 2002.

[5] Z.J. Haas, J.Y. Halpern, and L. Li. Gossip-based ad hoc routing. *IEEE/ACM Trans. Netw.*, 14(3):479–491, 2006.

[6] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4):660–670, October 2002.

[7] Y. Hu, A. Perrig, and D. Johnson. Wormhole detection in wireless ad hoc networks. Technical report, 2002.

[8] Y.C. Hu, A. Perrig, and D.B. Johnson. Wormhole detection in wireless ad hoc networks. Tech. Rep. TR01-384, Department of Computer Science, Rice University, June 2002.

[9] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 56–67, New York, NY, USA, 2000. ACM Press.

[10] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, May 2003.

[11] J. Kulik, W. Heinzelman, and H. Balakrishnan. Negotiation-based protocols for disseminating information in wireless sensor networks. *Wirel. Netw.*, 8(2/3):169–185, 2002.

[12] Arati Manjeshwar and Dharma P. Agrawal. Teen: Arouting protocol for enhanced efficiency in wireless sensor networks. In *IPDPS '01: Proceedings of the 15th International Parallel & Distributed Processing Symposium*, page 189, Washington, DC, USA, 2001. IEEE Computer Society.

[13] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler. Spins: security protocols for sensor networks. *Wirel. Netw.*, 8(5):521–534, 2002.

[14] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security: A survey, 2006.

[15] Y. Yu, R. Govindan, and D. Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. Technical report, 2001.