Design of Secure and Energy-Efficient Ad-Hoc Wireless Sensor Networks

Mukesh Singhal
Laboratory for Advanced Networking
Dept. of Computer Science
University of Kentucky
Lexington, KY 40506

Abstract: Wireless ad-hoc networks are vulnerable to several security threats. How to collect, exchange, and process data in a secure manner and reliably are key issues in such systems. At University of Kentucky, we are investigating security issues in wireless ad-hoc networks and this white paper will discuss initial results toward development of new methods for authentication for in-network data aggregation that will withstand various attacks,

1 Introduction

In recent years, there has been an increasing number of applications of cyber physical systems (CPSs) that use wireless ad-hoc networks to monitor and process real-time data that are spread in distributed environments. These applications include homecare medical assistance systems that monitor readings from sensors worn by people (e.g., blood pressure and heart rate) and sensors placed inside the living space, large-scale monitoring projects by environmental scientists, tracking applications that monitor locations of a number of objects, and a variety of safety, security and surveillance instances including transportation (e.g., air, rail, highways), public utilities (e.g., water, gas, electricity, nuclear power stations), buildings and gathering places (airports, train stations, shopping malls, football games), and military surveillance applications. Routing and data delivery in wireless ad-hoc networks are plagued with numerous security issues, like selective forwarding, sinkholes, HELLO floods, wormholes, bogus routing information and Sybil attacks [2, 3, 8]. How to collect, deliver, and process data in a secure and reliable manner key to the success of these applications.

At University of Kentucky, we are investigating some of the key issues in the security of ad-hoc wireless networks [1, 2, 3, 4, 5, 4, 6]. In this white paper, we discuss initial results for authentication for in-network data aggregation for energy-efficient secure transfer of data.

2 Security and Power Conservation in Robust Routing

Minimizing power consumption inherently improves the robustness of wireless ad-hoc networks by reducing node failure rate and maintaining connectivity of the network. Communication in wireless ad-hoc networks is an energy intensive operation. We are investigating power conservation in wireless ad-hoc networks by introducing the idea of in-network aggregation.

In-Network Aggregation Support for State-less Routing

With a state-less routing protocol, the process of data forwarding and routing are performed simultaneously and are not distinct processes. A node wishing to send data toward the base station selects a favorable neighbor based on attributes of the sensor nodes like geographical location and energy status and forwards data to the best candidate neighbor. However, current state-less routing protocols like IGF [9] and Feedback

Based Forwarding (FBF) [7] are not geared toward routing in presence of data aggregation. When in-network aggregation is desired, each intermediate node that forwards data for a neighbor must first convince all its other neighbors to forward their data through itself and then allow a sufficient wait time to gather all information from nodes to perform aggregation. To achieve this, we are building a state-less, or minimal state, routing protocol where, unlike in conventional state-less protocols, candidate neighbor selection not only depends on the most favorable attributes of a node but also on whether a node was previously selected by one of its other neighbors in the past. Also we are designing mechanisms that will allow a forwarding node to determine a suitable waiting period to gather all relevant data from neighbors without relying on any type of time synchronization mechanism that requires maintenance of state.

We are conducting research to address the following challenges: How do we build a routing protocol that supports in-network aggregation while requiring minimal state? In-network aggregation requires sensor nodes to be aware of an aggregating node. At the same time, an aggregating node needs to determine a suitable waiting period to gather all data from its neighbors before forwarding. State-less or minimal state routing in presence of data aggregation can be achieved through development of new techniques for selecting neighboring candidates to forward data, that leverage knowledge gained through passive listening, combined with techniques used in IGF and FBF.

Authentication for In-Network Aggregation

Routing in ad hoc networks is plagued with security issues [2, 3, 8]. Given low computation and communication capabilities along with limited energy resources available to mobile nodes, building security solutions to avoid these attacks becomes an increasingly challenging task. Since mobile nodes have performance constraints, cryptographic protocols must be lightweight requiring minimal processing and communication overhead, while maintaining a desired level of security. Only a handful of state-less secure routing protocols for ad-hoc sensor networks exist in the literature which include Secure Implicit Geographic Forwarding (SIGF) [10] and Feedback based Secure Routing (FBSR) [7]. Both these protocols have their drawbacks.

We are building a secure state-less, or at worst a minimal state, routing protocol that does not require a priori distribution of keys and extends hop-by-hop authentication to provide end-to-end authentication as well. Unlike prior secure state-less schemes like SIGF and FBSR, we are addressing significantly different routing objectives of routing in presence of in-network data aggregation and the resulting security problems. To address security issues, we will use MACs to provide authentication of data and develop techniques to prevent replay attacks without synchronization between nodes.

Assume sensor nodes are arranged in the form of a logical tree rooted at the base station. After a query is broadcast, a good practice is to allow nodes that are at the last hop from the base station (leaf nodes) to respond first and aggregate the data from intermediate nodes as it is propagated toward the base station. Traditional hop-by-hop authentication using MACs would cause a linear increase in communication and verification overhead as the data is propagated.

We advocate using aggregate MACs each internal node can combine its own MAC with the MACs of its children before sending the data toward the base station. If aggregation can be performed while maintaining the size of the MAC, then such a compression would reduce the communication overhead significantly. In addition, if the aggregation technique maintains the verification cost of the resulting MAC, then significant performance improvement can be achieved. Thus, aggregate MACs can be used to significantly improve communication and processing complexity in secure information aggregation schemes [11, 12, 13]. We have tackled a similar problem in the past relating to secure multicast feedback acknowledgement, and secure DSR, where we demonstrated a significant improvement in performance by using multisignatures [14, 15].

We are conducting research to address the following challenges:

- How can we build a MAC aggregation scheme where the verification cost is constant, irrespective of the number of participants? In the aforementioned scheme, verification costs increases linearly with the number of participants. While MAC aggregation techniques exist that result in constant verification cost, they often rely on expensive exponentiation operations.

- How can we build a MAC aggregation scheme where intermediate nodes can verify the *aggregate-so-far* MAC? The aforementioned scheme requires the base station to share a key with each node on the path that the data traverses and does not support verification at intermediate nodes.
- How do we bootstrap security in sensor networks? The bootstrap process involves distribution of keys to nodes in a secure manner, possibly establishing initial shared keys among nodes, and is essential for cryptographic authentication in sensor networks. Most secure routing schemes assume an out-of-band distribution of keys and pay little attention to this issue.

References

[1] Y. Sun, Q. Jiang, and M. Singhal, "An edge constrained localized delaunay graph for geographic routing in mobile ad hoc and sensor networks." to appear in IEEE Transactions on Mobile Computing.

[2] V. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," *Wireless Communications and Mobile Computing*, no. 6, pp. 1–24, 2006.

[3] S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks," *Ad Hoc Networks*, no. 1, pp. 151–174, 2003.

[4] V. C. Giruka, Y. Wang, and M. Singhal, "A secure position-based protocol framework for multi-hop ad-hoc networks," in *Proc. of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), October 8-10, White Plains, New York, USA*, 2007.

[5] R. Bai and M. Singhal, "DOA: DSR over AODV routing for mobile ad-hoc networks," *IEEE Transactions on Mobile Computing*, vol. 8, pp. 1403–1416, October 2006.

[6] H. Li and M. Singhal, "A secure routing protocol for wireless ad hoc networks," in *Proc. of 39th Hawaii International Conference on System Sciences (Minitrack on Security and Survivability of Unbounded Networked Systems), January, Hawaii, USA*, 2006.

[7] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "FBSR: Feedback based secure routing for wireless sensor networks," *Special Issue of International Journal of Pervasive Computing and Communication (JPCC)*, vol. 1, no. 4, 2008.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[9] B. Blum, T. He, S. Son, and J. Stankovic, "IGF: A state-free robust communication protocol for wireless sensor networks." Technical Report CS-2003-11, University of Virginia, VA, USA, 2003.

[10] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," in *Proceedings of SASN, 4th ACM Workshop on Security of ad hoc and Sensor Networks, Alexandria, VA, USA, October 30* (S. Zhu and D. Liu, eds.), pp. 35–48, ACM, 2006.

[11] J. Beaver, M. A. Sharaf, R. Labrinidis, and P. K. Chrysanthis, "Location-aware routing for data aggregation for sensor networks," in *In Proceedings of Geo Sensor Networks Workshop*, 2003.

[12] L. Hu and D. Evans, "Secure aggregation for wireless network," in *Proceedings of SAINT, Symposium on Applications and the Internet Workshops, Orlando, FL, USA, January 27-31*, pp. 384–394, IEEE Computer Society, 2003.

[13] B. Przydatek, D. X. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in *Proceedings of SenSys, 1st International Conference on Embedded Networked Sensor Systems, Los Angeles, CA, USA, November 5-7* (I. F. Akyildiz, D. Estrin, D. E. Culler, and M. B. Srivastava, eds.), pp. 255–265, ACM, 2003.

[14] S. Chakrabarti, S. Chandrasekhar, M. Singhal, and K. L. Calvert, "Authenticating feedback in multicast applications using a novel multisignature scheme based on cubic LFSR sequences," *AINAW: 21st International Conference on Advanced Information Networking and Applications Workshops*, vol. 1, pp. 607–613, 2007.

[15] S. Chakrabarti, S. Chandrasekhar, M. Singhal, and K. L. Calvert, "Authenticating DSR using a novel multisignature scheme based on cubic LFSR sequences," in *Proceedings of ESAS: The Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks* (F. Stajano, C. Meadows, and S. Capkun, eds.), vol. 4572 of *LNCS*, pp. 156–171, Springer, 2007.