RANDOMIZED ROUTES FOR SECURE DATA TRANSMISSION USING WIRELESS SENSOR NETWORKS

C.Muthuramalingam, A.Karthikeyan, R.Bharathiraj, M.Muthukummaar, S.Edwin Raja

P.S.R Engineering College, Sivaksi

ABSTRACT

Compromised node and denial of service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks. In this paper, we develop mechanisms that generate randomized multipath routes. Under our designs, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. We analytically investigate the security and energy performance of the proposed schemes. We also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints. Extensive simulations are conducted to verify the validity of our mechanisms.

Introduction

1.1 Scope of the Project

The main objective of this project is to provide security to the data transmission between source and destination sensor nodes by using ECDH security algorithm and, to avoid black holes.

1.2 WIRELESS SENSOR NETWORK

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. The more 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.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

1.3 Application of WSN:

1.3.1 Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

When the sensors detect the event being monitored (heat, pressure), the event is reported to one of the base stations, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can use a range of sensors to detect the presence of vehicles ranging from motorcycles to train cars.

1.3.2 Air pollution monitoring

Wireless sensor networks have been deployed in several cities (Stockholm, London or Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas. There are various architectures that can be used for such applications as well as different kinds of data analysis and data mining that can be conducted.

1.3.3 Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM)as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

1.3.4 Water/wastewater monitoring

There are many opportunities for using wireless sensor networks within the water/wastewater industries. Facilities not wired for power or data transmission can be monitored using industrial wireless I/O devices and sensors powered using solar panels or battery packs and also used in pollution control board.

3 Proposed System:

In this scheme a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible. Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost. By reducing hop count energy conservation can be avoided.

Advantages

- Purely random propagation (PRP), it utilizes only one-hop neighborhood information and pro-vides baseline performance
- Directed random propagation (DRP), it utilizes two-hop neighborhood information to improve the propagation efficiency, leading to a smaller packet interception probability
- Non repetitive random propagation (NRRP), scheme records all traversed nodes to avoid traversing them again in the future.
- Multicast tree-assisted random propagation (MTRP) it tries to propagate shares in the direction of the sink, making the delivery process more energy efficient.

Hardware and Software Specification: Processor: 1.4GHz Pentium IV Processor

- RAM : 128 MB
- Hard Drive : 10GB
- Operating System: Windows XP / Linux.
- Tools : ns-allinone-2.28.
- Pre-Request Software : Cygwin.
- Languages : Tcl/Tk, OTcl, C++.

Assumptions

The following simplifying assumptions are made in order to implement the mobile agent model.

1. Instead of sending the actual agent code along with data and execution stack, only a reference to the agent's OTcl object is sent. Thus, the actual sizes of agent's code, data and executi on state are required to be set as parameters of an agent. So it is assumed that all these parameters are known.

2. It is assumed that the servers, whose services are desired, are known in advance.

3. It is also assumed that the number of bytes required for request and reply in each interaction is known.

4. The processing time for an agent (if not explicitly specified for a specific scenario) and also the time for marshalling and unmarshalling are assumed to increase linearly with the total size of the agent.

5. The marshalling factor (marshalling ti me per unit byte) and time required for an agent's creation is assumed to be known.

6. The selectivity (Strasser pg. 18) of the mobile agent, defined as a factor by which the mobile agent reduces the size of the reply by remote processing, is also assumed to be known (if applicable).

7. No assumption is made about the underlying communication facilities for migrating agents. Any communication models including RPC, RMI, CORBA etc. can be utilized. But no such models are currently implemented in NS.

8. TCP is used as an underlying transport layer protocol. UDP may also be used here but the above choice is made only for the sake of performance analysis under reliable conditions.

9. As the principle aim of implementing this model is performance analysis of mobile agents, no consideration is given to the security matters in mobile agent systems. Thus, no security overhead is assumed.

10. Although implementation is bas ed upon an entry-point migration (Brewington pg. 15) (weak migration mainly using IBM's Aglets API), it is assumed to be equally applicable to t he study of agent systems with other types of migration using appropriate values for the model parameters. For example, while studying st rong migration, one can account for the size of agent's current execution stack, which can be otherwise considered as zero for weak migration.

Deciding the Inheritance Structure of the Model

In order to implement the basic behavioral model of mobile agent, the main objects required are a mobile agent itself and a context or a place where mobile agents can execute on a given node. Here, context is responsible for creating mobile agent and also for providing each and every facility required by the agent like dispatching to other node, loading and processing the incoming agent, registering, disposing etc. It uses the existing communication facilities for mobile agent migration. Thus, a context must be implemented on top of the transport layer facilities. Just like the real world systems, NS applications are implemented on top of the transport layer agents. Any simulated application is required to implement the Application interface provided in NS. Thus the mobile agent's context is required to implement this Application interface. Though context is implemented as an application, the mobile agent system model can be easily utilized for building real world applications on top of it.

System Architecture And Description

4 Wireless Channels

IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to the spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk and provide a noticeable performance increase over networks with minimal channel separation.

4.1 Wireless Sensor Network:

- Rapidly deployable, self configuring.
- No need for existing infrastructure.
- Wireless links.
- Senor nodes are mobile, topology can be very dynamic.
- Nodes must be able to relay traffic since communicating nodes might be out of range.

4.1.1 Sensor node usage areas:

The main two characteristics are mobility and multihop.

- Military scenarios
- Sensor networks
- Rescue operations
- Students on campus
- Free Internet connection sharing Conferences

4.1.2 Mechanisms required in a Senor Networks:

- Multihop operation requires a routing mechanism designed for mobile nodes.
- Internet access mechanisms.
- Self configuring networks requires an address allocation mechanism.
- Mechanism to detect and act on, merging of existing networks.
- Security mechanisms.

4.1.3 Routing protocol requirements:

- Self starting and self organizing
- Multi-hop, loop-free paths
- Dynamic topology maintenance
- Rapid convergence
- Minimal network traffic overhead
- Scalable to large networks

5 AES

5.1 Explanation:

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

6 Conclusion

By analyzing and simulating the results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters.The packet interception probability can be easily reduced by the new algorithms which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Specifically, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counter-parts. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels.

References

1. Ansgar Kellner, Kerstin Behrends, Dieter Hogrefe (2010) "Simulation Environments for Wireless Sensor Networks" TECHNICAL REPORT,IFI-TB-2010-04,JUNE 2010.

2. Sabitha Ramakrishna and T.Thyagarajan (2009) "Energy Efficient Medium Access Control for Wireless Sensor Networks" IJCSNS International Journal of Computer Science and Network Security,VOL.9 No.6,June 2009.

3. Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz (2008) "Security Issues in Wireless Sensor Networks" INTERNATIONAL JOURNAL OF COMMUNICATIONS, Issue 1, Volume 2, 2008.

4. A.Vijay kumar, T. Naveen, and B. Thirupathi (2011) "Secure Data Collection in Wireless Sensor Networks Using Randomized Routes" ARPN Journal of systems and software, Volume 1 No.5,August 2011.

5. Noor Zaman and Azween B Abdullah (2011) "Different Techniques Towards Enhancing Wireless Sensor Network (WSN) Routing Efficiency and Quality of service (QoS)" World Applied Sciences Journal 13(4);789-805,2011.ISSN 1818-4952 IDOSI publications,2011.

6. T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis,"Securing Wireless Sensor Networks Against Aggregator Compromises,"IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr.2008.

7. B. Vaidya, J.Y. Pyun, J.A. Park, and S.J. Han, "Secure Multipath Routing Scheme for Mobile Ad Hoc Network," Proc. IEEE Int'l symp. Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.

8. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR-a Secure Multipath Routing Protocol for Ad Hoc Networks," Ad-Hoc Networks, vol.5, no. 1, pp. 87-99, Jan. 2007.

9. P. Papadimitratos and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 343-356, Feb. 2006.

10. W. Lou and Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks" IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320-1330, July 2006.