Experimental Study on Secure Data Collection in Vehicular Sensor Networks

Harry Gao, Seth Utecht, Fengyuan Xu, Haodong Wang, and Qun Li

Department of Computer Science
College of William and Mary

Abstract. In this paper, we show through a simple secure symmetric key based protocol design and its implementation the feasibility of secure data collection in a vehicular sensor networks. We demonstrate that the protocol works in a realistic setting by collecting the real trace data through real implementation. Some of the key considerations are efficiency, deployability and security. The protocol does not safeguard against some of the techniques an adversary could deploy, such as jamming and deliberate battery-draining.

1 Introduction

We consider a simple vehicular network infrastructure composed of roadside sensors and the vehicles. Sensors are deployed to monitor road environment and the collected data can be collected by the vehicles passing by. In this network architecture, it is crucial to provide security support – only authorized vehicles can feed data into sensors and to obtain data from sensors. To block unauthorized and malicious vehicles, data collected by sensors must be encrypted. However, merely encrypting the data cannot prevent a malicious car to obtain the scrambled data. Although the encrypted data is of little use to the malicious vehicle, it is a serious problem when sensors expect vehicles to harvest all the data and carry them to a central station; a malicious vehicle can simply trap the data and leave a hole in the designated data repository. Therefore, authenticating a passing vehicle before transferring any data is indispensable.

A straightforward solution is to use a public-key based scheme, since some (e.g., the ECC) of the schemes can be implemented efficiently on sensor platforms. Taking a closer look at the problem in a real experimental study, we found that authentication takes about one to two seconds in many cases, which is non-negligible for a car traveling at tens meters a second. A car may rush out of a sensor's transmission range after the authentication is conducted. In this paper, we show our security solution to the vehicular sensor networks and give experimental results on a realistic deployment. We show through a simple secure protocol design and implementation the feasibility of secure data collection in a vehicular sensor networks. We deployed sensors along the road side to test the performance of the communication between the roadside sensors and the sensors in a moving vehicle. We demonstrate the protocol works in a realistic setting

B. Liu et al. (Eds.): WASA 2009, LNCS 5682, pp. 22–31, 2009.

by collecting the real trace data through real implementation. We hope this research shows valuable experience in deploying security support for this type of networks.

2 Related Work

A survey of the security of vehicular network can be found in [6]. There are many vulnerabilities for an unsecured network, such as jamming, forgery, impersonation, and in-transit traffic tampering [7]. Research shows that a symmetric key scheme is required [6]. A number of researching teams have put forth many solutions to group key and authentication problems [1] [2] [3] [8] [10]. Some of them utilize the Cabernet system where data is delivered opportunistically during travel. While less powerful, it does provide a quick solution that can be implemented without an overhaul [4] [5].

There have also been some research exploring the possibility of using a certificated-based protocol, such as the one proposed by Wang et al. [9]. It uses the short-range radio communication of motes to pass information from various roadside measuring devices to an information-gathering car mote, which then carries the information to a computer to process. However, it does not address some of the issues unveiled by Balfanz et al. [1].

3 Problem Setting

In this paper we assume the following environment and the availability of equipments:

- Many stationary sensors deployed on the side of the road that can detect, measure and record a certain aspect of the traffic pattern, such as the speed of vehicles in its range. Such motes are currently commercially available. It does not possess significant computational power, nor does it have much storage space.
- Another mote similar to the stationary ones placed in a car that can gather information from the stationary motes and then deliver it to a computer in the car. Its responsibility requires it to be able to securely communicate with other motes and with a computer.
- An upload server, which is to be located at the end of the road. It should be a computer with Wi-Fi capacity. It will obtain the relevant information from the computer in a car once in range. This upload server can be located in a toll gate, rest area, or any other similar structures. This server should have the ability to process and analyze the raw data, and notify relevant parties of its findings. As a computer, the upload server has much computational power. It is also assumed that its storage is virtually unlimited. This is justified by the fact it can communicate with external servers across the Internet. However, the upload server cannot communicate directly with the stationary motes.

– An authentication server, which is to be located at the beginning of the road. It should also be a computer with Wi-Fi capacity. It will permit the car mote to communicate with the stationary mote after the server verifies the car mote's identity. The exact protocol of authenticity between the car mote and authentication server is not discussed in this paper. This server, like the upload server, is assumed to have great computational power with virtually unlimited storage.

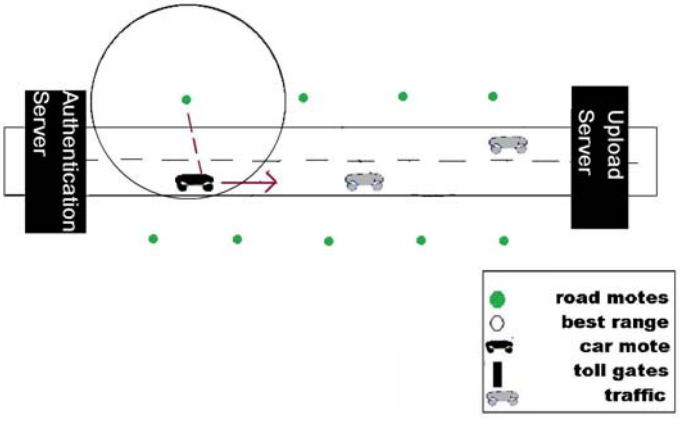

Fig. 1. A scenario of collecting data from roadside sensors in a vehicular networks

3.1 Adversary

Our goal is to design a protocol that is secure, reliable, and efficient. In the following we show our assumptions about the adversary.

The adversary is an unauthorized party that wishes to either obtain the secure information gathered by the roadside mote or at least block the car mote from gathering it. The adversary is assumed to have the ability unlimited access to any public information. It may try to impersonate the car mote so steal the data, or it may pretend to be a stationary roadside mote to provide the car mote with falsified data. Since the car mote is not a part of the infrastructure, it is even reasonable to assume that the car mote is malicious. However, this is not a major concern, since it is assumed that the authentication server will accurately identify any malicious parties before granting access. But in case the adversary successfully obtains the session key, it still cannot forge inaccurate data to the US, for it does not know the secret key.

The adversary is not expected to have the secret key, or know the hash function with which the secret message is encrypted. It is not able to physically damage any of the structures mentioned above, nor is it able to rewrite any pieces of software implemented on either the servers or the motes. That is, the adversary is an outside party without the knowledge of the inner workings of the system.

The adversary is also not expected to be able to crack the security via brute force. This assumption is reasonable since exemplary hashes are believed to be computationally infeasible to solve within any reasonable time frame [9].

4 Protocol

The following protocol is designed in order to balance security with efficiency. It provides a 3-key system that safeguards against various malicious parties, as well as a four-way handshake that allows the roadside mote and the info-gathering car mote to mutually authenticate. The symbols used in the protocol are summarized below:

Variable	Symbol
Car Mote	C
Roadside Mote	M
The secret massage	m
The authentication server	AS
The upload server	US
The session key generated by AS	k
Secret value known to M, AS and US	s
Randomly generated challenge value	r
Hash function of r and secret s	$hash(r,s)$
Random number used in the last step of verification	r_t

The first of the two servers provides car mote C with the necessary authentication information (denoted AS), while the second uploads and processes the data collected by C at the end of C's trip (denoted US. M wants to transfer data reliably to C as a car passes by. On the road, C will mutually authenticate with M and collect data encrypted with the secret key. At the end of the road, C will send all collected data to the upload server, which can use the secret key to decrypted the messages.

Pre-Distribution. The servers share the secret key s with M. No one else knows this key.

Communication between *AS* and *C*. To provide C the ability to access the information M holds, AS generates a random number R, and use this R to form a session key k:

$$k = hash(R, s) \tag{1}$$

AS performs this because it does not want C to know s, in order to prevent malicious C to forge fake sensors. After this process, AS gives k and R to C securely. C will now possess all the information it needs to collect data from M.

Communication between *C* and *M*. C broadcasts probe messages containing R on the road. When C and M are within the range of communication, M would receive the message and generate the session key $k = \text{hash}(s,R)$, which is the same key known to C. M can then perform a 4-way handshake with C:

1. M generates a random challenge r, and send it back to C;
2. C generates another random number R_c; compute a temporary key;

$$TK = hash(k, r, R_c) \tag{2}$$

   then it generates a MAC for R_c by using this TK; then sends both of them back to M
3. M compute the TK in the same way and use the key to verify the MAC. M can then send back another random number r_t with the MAC generated by using this TK. After verification, C will confirm that M get the TK correctly.
4. After that, both motes are authenticated with each other. M sends a success message and both sides can then start encrypted data communication.

Communication between *C* and the *US*. Upon arriving in the range of the upload server *US*, C uploads all gathered data as well as the session key to it for processing. *US* should have the ability to decrypt the encrypted information with the secret key, and it can verify with the AS that the session key is indeed a valid one. Once uploaded, C has finished its mission and can now reset.

Summery of the Protocol. The following figure summarizes the protocol outlined above.

```
AS to C    : R, k = hash(R,s)
C to M     : R
M computes : k = hash(R,s), generate r
M to C     : r
C computes : generate another random number R_c
           : TK = hash(k,r,R_c)
           : generate a MAC for R_c using TK
C to M     : MAC, R_c
M computes : TK in the same way; verify MAC, generate r_t
M to C     : MAC, r_t
C verifies : MAC; handshake complete
```

5 Experimental Results

To evaluate the proposed protocol, we have implemented it on two TelosB motes, one of them is used as M, while the other C. TelosB is powered by the MSP430 microcontroller. MSP430 incorporates an 8MHz, 16-bit RISC CPU, 48K bytes flash memory (ROM) and 10K RAM. The RF transceiver on TelosB is IEEE 802.15.4/ZigBee compliant, and can have 250kbps data rate. While the hardware directly affects the RSSI and other aspects of the experimental results, TelosB is by no mean the sole platform for the protocol is practical.

5.1 Metrics and Methodology

In this implementation, we used the following three metrics to better evaluate our results: received/dropped packets, received signal strength indication (RSSI), and the displacement across which the packets are transferred. On an open stretch of road, we drove past the roadside mote M at different speeds with the car mote C on top of the car and connected to a laptop (via USB), which runs a Java program that reads, records and analyzes the data received. M continually sent out radio transmissions in an infinite loop. Upon entering M's range, C picked up the encrypted message *hash(r,s)*, decrypted it and responded, and finally obtained the message m.

5.2 Mote to Mote Communication

Three distinct tests prove conducted. C is driven by M at the constant speed of 30, 50, and 70 km/h. Three trials were conducted for each speed. In addition, stationary tests at fixed displacements before and after M along the road were conducted at the displacements of 25, 75, 125, 175 and 225 meters. A unique ID number was assigned to every packet received for easier identification. The ID, the RSSI as well as the packet's time of arrive (an offset from the start time) were recorded for each trial. Also recorded was C's approximate displacement from M. From this, it was possible to calculate when, where, how many, and at what speed packets were dropped. The location of C along the road is expressed in terms of its displacement from M, where a negative value X represents that

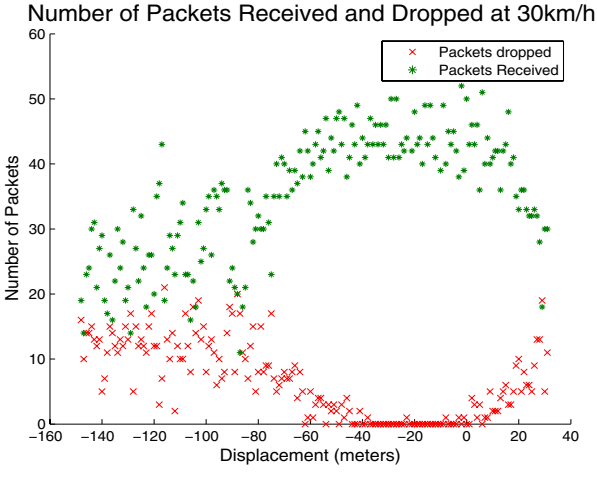

Fig. 2. This graph shows the number of packets received and dropped between the -150m and 50m, and it is the total of three separate trials. It shows that from about -40m to 0m, virtually all packets are successfully received for all three trials. It also shows that close to half of the packets are dropped near the ends of the graph.

C is X meters away from reaching the same point along the road as M, a value of 0 represent that it is at the exact same point along the road, and a positive value Y represent that C has passed M by Y meters.

In order to better analyze the relationship between possibility of dropping a package and the distance between the two motes, in figure 2, we graphed the total number of packets received/dropped for the three trials at 30km/h. From the graph, it is evident that at the possible range for C to receive packets from M is around between -150 meters and 50 meters. This represents a window of opportunity of about 200 meters, or about 24 seconds. However, significant number of packets was dropped from -155 meters to about -55 meters, and again resumes to drop significantly at around 25 meters. Therefore, the most reliable window of communication where very few packets (less than 5 percent) is around -55 meter to 25 meters. This 80 meter window represent about 10 seconds.

The data of 50 km/h and 70 km/h show a similar pattern. However, the optimal window of transmission is halved to just under 6 seconds. This could be too short to fully and securely transfer all data based on the currently protocol. The possible range of reception, optimal range of reception and approximate time frame to transfer data within the two ranges are summarized in the table below:

Analysis of Possible/Best Packet Transmission Frames

Car Speed	Possible Range	Optimal Range	Possible Duration	Optimal Duration
km/h	meters	meters	seconds	seconds
30	[-150, 50]	[-55, 25]	24	10
50	[-150, 50]	[-75, 5]	14	5.8
70	[-150, 50]	[-85, 25]	10	5.7

The table is populated with the average of the three trials for each speed. Possible range represents all displacement values where transmission is possible, whereas the optimal range represent the best range for transmission as discussed above. We can use our knowledge of the best window of communication to increase the reliability of our protocol. Possible/optimal duration represents the amount of time in seconds C will stay in the respective ranges.

5.3 RSSI

The signal strength (RSSI) is plotted against displacement in figure 3 to better analyze the relationship between the two. Three trials show an identical trend with slight horizontal displacement. The signal strength for the first trial peaked at about -13 meters, second trial at -5 meters, while the third one peaked at -26 meters. It is, however, clear from the graph that RSSI increases as the displacement narrows. The fact all three trials peaked at slightly negative displacement suggests that the radio signals are stronger before C passes M. However, there is little difference between about -175 meters and -75 meters in terms of RSSI, suggesting that the strength is not simply inversely proportional to the displacement. This information provides insight to the best timing of the handshake

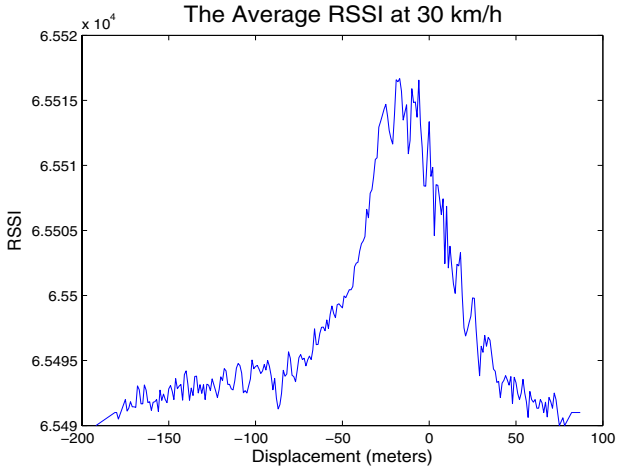

Fig. 3. The RSSI of the packets received within [-200m, 80m]. At about 50m away from the roadside mote the transmission becomes reliable, until it passes the roadside mote by about 25 meters. It peaks shortly before reaching 0m.

process, and we can use the RSSI as an indicator to show if the communication strength is high enough for the security protocol to start. At 50km/h and 70km/h, a similar pattern is shown. The results are summarized below:

Approx. Displacement of Best RSSI

Car Speed	Displacement	Time
30 km/h	-8 meters	-1.0 sec
50 km/h	-16 meters	-1.2 sec
70 km/h	-23 meters	-1.2 sec

The trend shows that as speed of the vehicle hosting C increases, the ideal displacement from M for packet transmission becomes increasingly negative. The ideal amount of time for packet transmission, on the other hand, seems to be about just more than 1.0 seconds regardless of the difference in speed.

5.4 Security

The amount of time authentication of this protocol takes is compared with other schemes in order to better analyze the efficiency and dependability of the protocol. In particular, the amount of time needed to encrypt the message with AES takes less than 1ms with 16 byte-long keys and random numbers. SHA-1 would take 4ms. The proposed protocol can use either one of those two. The speed of encryption/decryption is extremely important in the context. This is because the car mote only has about 6 seconds to communicate with a roadside mote at high speed, and we must ensure not only that we have enough time for the handshake, but also that the security part takes only a small fraction of the amount of time we have, and that sufficient amount of time is left for the actual data to pass through. On

the same platform, we found that the ECC-based encryption needs 2 point multiplications, which takes roughly 3.1 seconds on the TelosB. Decryption will take one point multiplication, or about 1.55 seconds. This suggests that an asymmetric key scheme would take much longer to establish the secured connection and is not be suitable for a similar set up. Using the symmetric key protocol as proposed, the total amount of time needed for the motes to encrypt/decrypt is negligible. In addition to the calculation time, however, we also need to consider the amount of time it takes to actually transmit handshake messages. The protocol requires a 4-way handshake, 2 packets to be sent from the car mote to the roadside mote, and 2 more going the other way. At the experimental rate of 13 packets per second on average, the communication will take roughly 0.31s. Therefore, the total amount of time required for the authentication is about one third of a second, or less than 5 percent of the total amount of available time inside the optimal transmission range. This is very acceptable.

5.5 Further Observation

At high speed, there would be about 6.5 seconds left for the transferring of interesting data. The TelosB hardware has a maximum transfer rate of 250kbps (as declared on its specifications) and an experimental rate of 200kbps at 70km/h. This means that it will take about 6 cars to unload all 1024K bytes of data the hardware can hold at a time. However, in a realistic setting, we should extract the data long before the on board flash memory is full. The low percentage of communication time shows the protocol is useful in a realistic setting. In the experiment we did not try to tweak the packet size to maximize the amount of data transferred at a time; ideally, we should be able to reach the rate of 250kbps, and only five car motes need to drive by to collect all data resting on the roadside mote.

6 Conclusion

In this paper, we show our design of a secure data collection protocol for vehicular sensor networks. We conducted experimental study on this protocol. There are many interesting findings in this implementation. First of all, it shows that many of the goals of vehicular network communication can be easily achievable. At a speed as high as 70 km/h, the motes still have about 5.7 seconds of optimal transmission time, which should suffice under normal circumstances. Another interesting conclusion drawn from the data is that the signal strength is better when C is still some distance away from M than when the two are at the same point along the road. This is confirmed by the fact the optimal range of transmission is not centered at a displacement of 0 meters, but at around -30 to -15 meters.

Acknowledgments

This project was supported in part by US National Science Foundation grants CNS-0721443, CNS-0831904, CAREER Award CNS-0747108, and CSUMS grant DMS 0703532.

References

1. Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddonand, J., Wong, H.C.: Secret handshakes from pairing-based key agreements. In: IEEE Symposium on Security and Privacy, pp. 180–196 (2003)
2. Chan, H., Perrig, A.: Pike: peer intermediaries for key establishment in sensor networks. In: INFOCOM, pp. 524–535 (2005)
3. Du, W., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, pp. 586–597 (2004)
4. Eriksson, J., Balakrishnan, H., Madden, S.: Cabernet: vehicular content delivery using Wi-Fi. In: MOBICOM (2008)
5. David, H., Srinivasan, K., Tim, B., Shubham, A.: Vehicular opportunistic communication under the microscope. In: MobiSys 2007: Proceedings of the 5th international conference on Mobile systems, applications and services, New York, NY, USA, pp. 206–219 (2007)
6. Luo, J., Hubaux, J.-P.: A survey of inter-vehicle communication, epfl. Technical report (2004)
7. Raya, M., Papadimitratos, P., Hubaux, J.P.: Securing vehicular communications. In: IEEE Wireless Comm. (2006)
8. Vogt, H.: Exploring message authentication in sensor networks. In: Castelluccia, C., Hartenstein, H., Paar, C., Westhoff, D. (eds.) ESAS 2004. LNCS, vol. 3313, pp. 19–30. Springer, Heidelberg (2005)
9. Wang, H., Li, Q.: Distributed user access control in sensor networks. In: Gibbons, P.B., Abdelzaher, T., Aspnes, J., Rao, R. (eds.) DCOSS 2006. LNCS, vol. 4026, pp. 305–320. Springer, Heidelberg (2006)
10. Zhu, S., Setia, S., Jajodia, S.: An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In: IEEE Symposium on Security and Privacy, pp. 259–271 (2004)