International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 1, Volume 2 (January 2015) www.ijirae.com

Privacy Preserving Protocol to collect without identity of the Aggregate nodes

N.K.Prema,
Research Scholar/CSE
PRIST University,
Thanjavur,Tamil Nadu

Dr.A.Arul Lawrence S.K
Professor /CSE
Rajiv Gandhi Institute of Technology
Bangalore -32

Abstract: Wireless networks are used in our everyday life. We use wireless networks to call each other, to download our emails at home, or to enter a building with a proximity card. In the near future wireless networks will be used in many new fields such as vehicular ad hoc networks, or critical infrastructure protection. The use of wireless networks instead of wired networks opens up new research challenges. These challenges include mobility, coping with unreliable links, resource constraints, and the security and privacy aspects of the wireless networks. In this paper some privacy aspects of different wireless networks are investigated. In private authentication methods are proposed and analyzed for radio frequency identification (RFID) systems. A typical example for such an application is a Radio Frequency Identification System (RFID) system, where the provers are low-cost RFID tags, and the number of the tags can potentially be very large. I study the problem of private authentication in RFID systems. More specifically I propose two methods, that are the privacy efficient key-tree based authentication, and the group based authentication. The first key-tree based private authentication protocol has been proposed by Molnar and Wagner as a neat way to efficiently solve the problem of privacy preserving authentication based on symmetric key cryptography. However, in the key-tree based approach, the level of privacy provided by the system to its members may decrease considerably if some members are compromised. In this paper, I analyze this problem, and show that careful design of the tree can help to minimize this loss of privacy. First, I introduce a benchmark metric for measuring the resistance of the system to a single compromised member. This metric is based on the well-known concept of anonymity sets. Then, I show how the parameters of the key-tree should be chosen in order to maximize the system's resistance to single member compromise under some constraints on the authentication delay. In the general case, when any member can be compromised, I give a lower bound on the level of privacy provided by the system. I also present some simulation results that show that this lower bound is quite sharp. The results can be directly used by system designers to construct optimal key-trees in practice.

Keywords: wireless Networks, Sensor Networks.

1. INTRODUCTION

I propose a novel group based authentication scheme similar to the key-tree based method. This scheme is also based on symmetric-key cryptography, and therefore, it is well-suited to resource constrained applications in large scale environments. I analyze the proposed scheme and show that it is superior to the previous key-tree based approach for private authentication both in terms of privacy and efficiency.

I analyze the privacy consequences of inter vehicular communication. The promise of vehicular communications is to make road traffic safer and more efficient. However, besides the expected benefits, vehicular communications also introduce some privacy risk by making it easier to track the physical location of vehicles. One approach to solve this problem is that the vehicles use pseudonyms that they change with some frequency. In this chapter, I study the effectiveness of this approach. I define a model based on the concept of mix zone, characterize the tracking strategy of the adversary in this model, and introduce a metric to quantify the level of privacy enjoyed by the vehicles. I also report on the results of an extensive simulation where I used my model to determine the level of privacy achieved in realistic scenarios. In particular, in my simulation, I used a rather complex road map, generated traffic with realistic parameters, and varied the strength of the adversary by varying the number of her monitoring points. My simulation results provide information about the relationship between the strength of the adversary and the level of privacy achieved by changing pseudonyms. It can be seen that untraceability of vehicles is an important requirement in future vehicle communications systems. Unfortunately, heartbeat messages used by many safety applications provide a constant stream of location data, and without any protection measures, they make tracking of vehicles easy even for a passive eavesdropper.

However, considering a global attacker, this approach is effective only if some silent period is kept during the pseudonym change and several vehicles change their pseudonyms nearly at the same time and at the same location. Unlike other works that proposed explicit synchronization between a group of vehicles and/or required pseudonym change in a designated physical area (i.e., a static mix zone), I propose a much simpler approach that does not need any explicit cooperation between vehicles and any infrastructure support. My basic idea is that vehicles should not transmit heartbeat messages when their speed drops below a given threshold, and they should change pseudonym during each such silent period.

This ensures that vehicles stopping at traffic lights or moving slowly in a traffic jam will all refrain from transmitting heartbeats and change their pseudonyms nearly at the same time and location. Thus, my scheme ensures both silent periods and synchronized pseudonym change in time and space, but it does so in an implicit way. I also argue that the risk of a fatal accident at a slow speed is low, and therefore, my scheme does not seriously impact safety-of-life.

In addition, refraining from sending heartbeat messages when moving at low speed also relieves vehicles of the burden of verifying a potentially large amount of digital signatures, and thus, makes it possible to implement vehicle communications with less expensive equipments. I propose protocols that increase the dependability of wireless sensor networks, which are potentially useful building blocks in cyber-physical systems. Wireless sensor networks can be used in many critical applications such as martial or critical infrastructure protection scenarios. In such a critical scenario, the dependability of the monitoring sensor network can be crucial. One interesting part of the dependability of a network, is how the network can hide its nodes with specific roles from an eavesdropping or active attacker.

In this problem field, I propose protocols which can hide some important nodes of the network. More specifically, I propose two privacy preserving aggregator node election protocols, a privacy preserving data aggregation protocol, and a corresponding privacy preserving query protocol for sensor networks that allow for secure in-network data aggregation by making it difficult for an adversary to identify and then physically disable the designated aggregator nodes. The basic protocol can withstand a passive attacker, while my advanced protocols resist strong adversaries that can physically compromise some nodes. The privacy preserving aggregator protocol allows electing aggregator nodes within the network without leaking any information about the identity of the elected node. The privacy preserving aggregation protocol helps collecting data by the elected aggregator nodes without leaking the information, which is actually collecting the data. The privacy preserving query protocol enables an operator to collect the aggregated data from the unknown and anonymous aggregators without leaking the identity of the aggregating nodes

II. RESULT FINDINGS

In this paper three different wireless network based systems are considered: Radio Frequency Identification Systems, Vehicular Ad Hoc Networks, and Wireless Sensor Networks. In this chapter, a brief overview is give, where these systems are used, and how my new results fit in them.

Radio Frequency Identification Systems The application of RFID is very widespread, some application areas are [Wu *et al.*, 2014; RFID, 2014]:
Payment by mobile phones Many companies like MasterCard or Nokia is working on mobile phones with embedded RFID capabilities to enable payment by such devices.

Inventory systems RFID systems can provide accurate knowledge of the current inventory, which helps saving labor cost, and enables self checkout in shops.

Access control RFID tags can be used as identification badges to enable access control in office buildings, or can be used as tickets in automated fare collection systems.

Transportation and logistics In transportation, RFID tags can help identify cargo, its owner or destination.

Passport Many countries include RFID tags into passports, to fasten the passport control on the borders, and to make illegitimate replication harder.

Hospitals and healthcare Hospitals began implanting patients with RFID tags and using RFID systems, usually for workflow and inventory management [Fisher, 2014].

Libraries Libraries are using RFID to replace the barcodes on library items. An RFID system may replace or supplement bar codes and may offer another method of inventory management and self-service checkout by patrons. [Molnar and Wagner, 2014] Any usage of RFID systems, where the holder of the tag is a human being might breach the privacy of the holder. The solutions proposed in Chapter 2 can be used in such situations. An example application is the automated fare collection systems, where the pass for the mass transportation system can contain an RFID tag. In such a system, the system designer might consider the usage of key trees or group based private authentication, in particular if the legal environment requires the usage of some kind of privacy enhancing technology.

Vehicular Ad Hoc Networks The application of Vehicular Ad Hoc Networks is very widespread, but can be categorized into three main categories: safety related applications, transport efficiency, and information/entertainment applications [Hartenstein and Laberteaux, 2013; Willke *et al.*, 2014].

Hundreds of possible applications can be envisioned or are under construction. Such an application is the cooperative forward collision warning, which help avoiding rear-end collisions with the use of beacon messages. The traffic efficiency for example can be increased by a traffic light optimal speed advisory application, which can assists the driver to arrive during a green phase. An example for the information gathering applications is the ability of remote wireless diagnosis, which enables to make the state of the vehicle accessible for remote diagnosis. Most of the safety and traffic efficiency related applications are based on the beacon messages, which are frequent messages containing the location, heading, identifier, and some other attributes of the vehicle. These messages can enable the tracking of individual vehicles, which is an undesirable side effect of the usage of VANETs. This side effect is analyzed in Chapter 3, and a countermeasure is proposed as well. The countermeasure algorithm is compatible with the framework proposed by the Car 2 Car Communication Consortium [Consortium, 2015].

Most of the results of Chapter 3 were parts of the results of the SeVeCom1 European Commission funded project. The results were delivered to and accepted by the European Commission.

Wireless Sensor Networks Wireless sensor networks can be used in many scenarios. In Chapter 4 I proposed two anonym aggregation schemes, which hides the identity of the aggregator node. In the following a few applications are given based on with a special attention on the possible need of hiding some special nodes: wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems, where there is a clear motivation for an attacker to disturb the normal functioning of the network by eliminating some special nodes. Another example can be the protection of critical infrastructure. The problem is that some critical infrastructure like electrical lines or drinking water pipes are so large scale, that it is impossible to protect them with traditional methods. WSNs can be a possible protection and surveillance system, where the disturbance of normal operation by the elimination of aggregator nodes must be avoided. In the above mentioned applications, there is a clear need for aggregation, and the loss of the aggregator might have undesirable consequences. Hence in these applications, the anonym aggregator election, aggregation, and query schemes proposed in Chapter 4 can be used. The goal of the Wireless Sensor and Actuator Networks for Critical Infrastructure Protection project (WSAN4CIP2), funded by the European Commission, was to make critical infrastructure more dependable by the use of WSNs. Some of the results of Chapter 4 were integral part of that project.

III. RESULT

In this paper, I proposed several privacy enhancing protocols for wireless networks. I dealt with three different types of networks, namely RFID systems, vehicular ad hoc networks, and wireless sensor networks. I proposed a key-tree and a group based private authentication protocol for RFID systems. Both approaches use only symmetric key based cryptographic primitives, which well suits to resource limited RFID systems. Key-trees provide an efficient solution for private authentication, however, the level of privacy provided by key-tree based systems decreases considerably if some members are compromised. This loss of privacy can be minimized by the careful design of the tree. Based on my results presented in this paper, I can conclude that a good practical design principle is to maximize the branching factor at the first level of the tree such that the resulting tree still respects the constraint on the maximum authentication delay in the system. Once the branching factor at the first level is maximized, the tree can be further optimized by maximizing the branching factors at the successive levels, but the improvement achieved in this way is not really significant; what really counts is the branching factor at the first level.

I proposed a novel group based private authentication scheme. I analyzed the proposed scheme and quantified the level of privacy that it provides. I compared my group based scheme to the key-tree based scheme. I showed that the group based scheme provides a higher level of privacy than the key-tree based scheme. In addition, the complexity of the group based scheme for the verifier can be set to be the same as in the key-tree based scheme, while the complexity for the prover is always smaller in the latter scheme. The primary application area of my schemes are that of RFID systems, but it can also be used in applications with similar characteristics (e.g., in wireless sensor networks).

Some possible work that could be done is the usage of different metrics like the entropy based metric, or the usage of different constraints like the minimal size of the anonymity sets when selecting a structure like the groups for the users. These new metrics or constraints can make the resulting optimization problem complex, which can require heuristic solutions as well. A general framework that could solve the optimization problem for different metrics and constraints could be a future research direction.

The most criticized part of any key tree or group based solution is the difficulty of the key update. Hence, a challenging future work could be the implementation of a key update scheme in a tree based solution. I studied the effectiveness of changing pseudonyms to provide location privacy for vehicles in vehicular networks. The approach of changing pseudonyms to make location tracking more difficult was proposed in prior work, but its effectiveness has not been investigated yet.
In order to address this problem, I defined a model based on the concept of the mix zone. I assumed that the adversary has some knowledge about the mix zone, and based on this knowledge, she tries to relate the vehicles that exit the mix zone to those that entered it earlier. I also introduced a metric to quantify the level of privacy enjoyed by the vehicles in this model. In addition, I performed extensive simulations to study the behavior of my model in realistic scenarios. In particular, in my simulation, I used a rather complex road map, generated traffic with realistic parameters, and varied the strength of the adversary by varying the number of her monitoring points. My simulation results provided detailed information about the relationship between the strength of the adversary and the level of privacy achieved by changing pseudonyms. I abstracted away the frequency with which the pseudonyms are changed, and I simply assumed that this frequency is high enough so that every vehicle surely changes pseudonym while in the mix zone. It seems that changing the pseudonyms frequently has some advantages as frequent changes increase the probability that the pseudonym is changed in the mix zone. On the other hand, the higher the frequency, the larger the cost that the pseudonym changing mechanism induces on the system in terms of management of cryptographic material (keys and certificates related to the pseudonyms). In addition, if for a given frequency, the probability of changing pseudonym in the mix zone is already close to 1, then there is no sense to increase the frequency further as it will no longer increase the level of privacy, while it will still increase the cost. Hence, there seems to be an optimal value for the frequency of the pseudonym change.

Unfortunately, this optimal value depends on the characteristics of the mix zone, which is ultimately determined by the observing zone of the adversary, which is not known to the system designer. I proposed a simple and effective privacy preserving scheme, called SLOW, for VANETs. SLOW requires vehicles to stop sending heartbeat messages below a given threshold speed (this explains the name SLOW that stands for “silence at low speeds”) and to change all their identifiers (pseudonyms) after each such silent period. By using SLOW, the vicinity of intersections and traffic lights become dynamically created mix zones, as there are usually many vehicles moving slowly at these places at a given moment in time. In other words, SLOW implicitly ensures a synchronized silent period and pseudonym change for many vehicles both in time and space, and this makes it effective as a location privacy enhancing scheme. Yet, SLOW is remarkably simple, and it has further advantages. For instance, it relieves vehicles of the burden of verifying a potentially large amount of digital signatures when the vehicle density is large, as this usually happens when the vehicles move slowly in a traffic jam or stop at intersections. Finally, the risk of a fatal accident at a slow speed is low, and therefore, SLOW does not seriously impact safety-of-life. I evaluated SLOW in a specific attacker model that seems to be realistic, and it proved to be effective in this model, reducing the success rate of tracking a target vehicle from its starting point to its destination down to the range of 10–30%. Some future work could be a detailed analysis of the result of SLOW on the safety of vehicles, or the analysis of the exceptional cases where the vehicles are forced to send a beacon message below the threshold.

I proposed two private aggregation algorithms for wireless sensor networks. In wireless sensor networks, in-network data aggregation is often used to ensure scalability and energy efficient operation. However, this also introduces some security issues: the designated aggregator nodes that collect and store aggregated sensor readings and communicate with the base station are attractive targets of physical node destruction and jamming attacks. In order to mitigate this problem, I proposed two private aggregator node election protocols for wireless sensor networks that hide the elected aggregator nodes from the attacker, who, therefore, cannot locate and disable them. My basic protocol provides fewer guarantees than my advanced protocol, but it may be sufficient in cases where the risk of physically compromising nodes is low. My advanced protocol hides the identity of the elected aggregator nodes even from insider attackers, thus it handles node compromise attacks too. I also proposed a private data aggregation protocol and a corresponding private query protocol for the advanced version, which allow the aggregator nodes to collect sensor readings and respond to queries of the operator, respectively, without revealing any useful information about their identity.

IV.CONCLUSION

My aggregation and query protocols are resistant to both external eavesdroppers and compromised nodes participating in the protocol. The communication in the advanced protocol is based on the concept of connected dominating set, which suits well to wireless sensor networks. I went beyond the goal of only hiding the identity of the aggregator nodes. I also analyzed what happens if a malicious node wants to exploit the anonymity offered by the system, and tries to mislead the operator by injecting false reports. I proposed an algorithm that can detect if any of the nodes misbehaves in the query phase. I only detect the fact of misbehavior and leave the identification of the misbehaving node itself for future work. A more challenging future work is the reduction of the message or computational complexity of the election subprotocol.

V.REFERENCE

[1]. M. Abadi and C. Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, 2004.
[2]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2013.
[3]. R. Anderson and M. Kuhn. Tamper resistance: a cautionary note. In *Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce-Volume 2*, page 1. USENIX Association, 2009.
[4]. M. Aoki and H. Fujii. Inter-vehicle communication: Technical issues on vehicle control application. *Communications Magazine, IEEE*, 34(10):90–93, 2011.
[5]. A.R. Beresford and F. Stajano. Mix zones: User privacy in locationaware services. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 127–131. IEEE, 2014.
[6]. Z. Berki. *Development of Traffic Models on the basis of Passanger Demand Surveys Paper of the PhD dissertation*. PhD paper, Budapest University of Technology and Economics, 2014.
[7]. M. Beye and T. Veugen. Improved anonymity for key-trees? Technical report, Cryptology ePrint Archive, Report 2011/395, 2013.
[8]. M. Beye and T. Veugen. Anonymity for key-trees with adaptive adversaries. *Security and Privacy in Communication Networks*, pages 409–425, 2013.
[9]. Jan Camenisch and Markus Stadler. Proof systems for general statements about discrete logarithms. Technical report, Department of Computer Science, ETH Z¨urich, 2010.
[10]. B. Carbunar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan. Query privacy in wireless sensor networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pages 203–212. IEEE,2012.
[11]. H. Chan and A. Perrig. Security and privacy in sensor networks. *Computer*, 36(10):103–105, 2013.
[12]. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, pages 197–215. IEEE Computer Society, 2013.

