IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 3, 2015, Page.1006-1012, ISSN: 2347–8586

A Strong Key Pre Distribution Scheme for Wireless Sensor Networks

Rajender Gajula[1] and A Balaram[2]
[1]Assistant Professor, [2]Associate Professor
Department of Computer Science and Engineering,
KITE College of Professional Engineering Sciences, Telangana, India

ABSTRACT: Given the sensitivity of the potential WSN applications and because of resource limitations, key management emerges as a challenging issue for WSNs. One of the main concerns when designing a key management scheme is the network scalability. Indeed, the protocol should support a large number of nodes to enable a large scale deployment of the network. In this paper, a new scalable key management scheme for WSNs which provides a good secure connectivity coverage. For this purpose, the make use of the unital design theory. It show that the basic mapping from unitals to key pre-distribution allows us to achieve high network scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, it propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability approximately lower bounded by $1 - e^{-1} \approx 0.632$. It conduct approximate analysis and simulations and compare our solution to those of existing methods for different criteria such as storage overhead, network scalability, network connectivity, average secure path length and network resiliency. Our results show that the proposed approach enhances the network scalability while providing high secure connectivity coverage and overall improved performance. Moreover, for an equal network size, our solution reduces significantly the storage overhead compared to those of existing solutions.

1. Introduction

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. 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[2]. 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. in VANET, our project is concerned only with the location privacy and traceability.

1.1 APPLICATIONS

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 detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

Environmental/Earth monitoring

The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests, etc. Some of the major areas are listed below.

Air quality monitoring

The degree of pollution in the air has to be measured frequently in order to safeguard people and the environment from any kind of damages due to air pollution. In dangerous surroundings, real time monitoring of harmful gases is an important process because the weather can change rapidly changing key quality parameters.

- **Interior monitoring**

Observing the gas levels at vulnerable areas needs the usage of high-end, sophisticated equipment, capable to satisfy industrial regulations. Wireless internal monitoring solutions facilitate keep tabs on large areas as well as ensure the precise gas concentration degree.

- **Exterior monitoring**

External air quality monitoring needs the use of precise wireless sensors, rain & wind resistant solutions as well as energy reaping methods to assure extensive liberty to machine that will likely have tough access.

Air pollution monitoring

Wireless sensor networks have been deployed in several cities (Stockholm, London and 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.

Forest fire detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the fire fighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

Water quality monitoring

Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.

Natural disaster prevention

Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.

Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality. 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.

Data logging

Main article: Data logging

Wireless sensor networks are also used for the collection of data for monitoring of environmental information; this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.

1.3. Project organization

The remaining section of the project is organized as follows: the related work to this project is addressed in section 2. The overview of the project is discussed in section 3 and the efficient authentication method that ensures location privacy of the vehicle is briefly explained in section 4. The performance analysis of the proposed work is performed in section 5 and the project is concluded in section 6.

2. Related works

A. Securing wireless sensor networks: a survey

The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network. WSNs have attracted intensive interest from both academia and industry due to their wide application in civil and military scenarios. In hostile scenarios, it is very important to protect WSNs from malicious attacks. Due to various resource limitations and the salient features of a wireless sensor network, the security design for such networks is significantly challenging. In this article, it present a comprehensive survey of WSN security issues that were investigated by researchers in recent years and that shed light on future directions for WSN security[1].

B. A key-management scheme for distributed sensor networks

Distributed Sensor Networks (DSNs) are ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. DSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. DSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of communications, sensorcapture detection, key revocation and sensor disabling. In this paper, it present a key-management scheme designed to satisfy both operational and security requirements of DSNs[2].

C. Random key predistribution schemes for sensor networks

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. We present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key predistribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, we present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation [3].

D. A key management scheme for wireless sensor networks using deployment knowledge

To achieve security in wireless sensor networks, it is important to be able to encrypt messages sent among sensor nodes. Keys for encryption purposes must he agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. Recently, a random key pre-distribution scheme and its improvements have been proposed.

A common assumption made by these random key pre-distribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori, we propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. We show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can he substantially improved with the use of our proposed scheme. The scheme and its detailed performance evaluation are presented in this paper[4].

3. EXISTING SYSTEM

Wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pair wise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution[5].

4. PROPOSED SYSTEM

In this proposed system, our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, we make use, of the unital design theory for efficient WSN key pre-distribution.

ADVANTAGES OF PROPOSED SYSTEM

The advantages of the proposed system as follows:

- We propose a naive mapping from unital design to key pre-distribution and we show through analytical analysis that it allows to achieve high scalability.
- We propose an enhanced unitalbased key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability.
- We analyze and compare our new approach against main existing schemes, with respect to different criteria: storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency.

4.1 System model

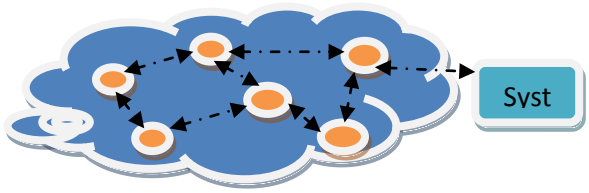

Figure 1. Architecture

4.2 Goals

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.

6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

5. Implementation

Modules

1. Node Deployment
2. Key Generation
3. Key Pre-distribution Technique
4. Secure Transmission with Energy

Node Deployment

The first module is Node deployment, where the node can be deployed by specifying the number of nodes in the network. After specifying the number of nodes in the network, the nodes are deployed. The nodes are deployed with unique ID (Identity) number so that each can be differentiated. And also nodes are deployed with their energy levels.

Key Generation

After the Node deployment module, the key generation module is developed. Where the number of nodes and number of blocks should be specified, so that the key will be generated. The key is symmetric key and the key is displayed in the text area given in the node.

Key Pre-distribution Technique:

In this module, we generate blocks of m order initial design, where each block corresponds to a key set. We pre-load then each node with t completely disjoint blocks where t is a protocol parameter that we will discuss later in this section. In lemma 1, we demonstrate the condition of existence of such t completely disjoint blocks among the unital blocks. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key. Contrary to this, pre-loading each two nodes with t disjoint unital blocks means that each two nodes share between zero and keys since each two unitals blocks share at most one element. After the deployment step, each two neighbors exchange the identifiers of their keys in order to determine the common keys. This approach enhances the network resiliency since the attackers have to compromise more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links.

Secure Transmission with Energy

In this module, the node distance is configured and then the nodes with their neighbor information are displayed. So the nodes which is near by the node, is selected and the energy level is first calculated to verify the secure transmission. After that the data is uploaded and sent to the destination node. Where in the destination node, the key is verified and then the data is received.

5.2 PERFORMANCE COMPARISON

In this section, we compare the proposed unital-based schemes to existing schemes regarding different criteria.

5.2.1 Network scalability at equal key ring size

The scalability of the proposed unital based schemes against that of the SBIBD-KP and the Trade-KP ones. The network scalability of the t-UKP schemes is computed as the average value between the maximum and the minimum scalability. The network scalability of the SBIBD-KP scheme is computed as $m2 + m + 1$ where m is the SBIBD design order and $m + 1$ is the key ring size. We compute the salability of the Trade-KP scheme as $2q2$ where q is the first prime power greater than the key ring size k, this value allows a achieve the best session key sharing probability using the Trade-KP scheme as we proved in [13] The figure shows that at equal key ring size, the NU-KP scheme allows to enhance greatly the scalability compared to the other schemes; for instance the increase factor reaches 10000 compared to the SBIBD-KP scheme when the key ring size exceeds 100.

Moreover, the figure shows that the t-UKP schemes achieve a high network scalability. We notice that the higher t is, the lower network scalability is. Nevertheless, 2- UKP and 3-UKP give better results than those of the SBIBDKP and the Trade-KP solutions. Even we choose $t = \sqrt{m}$ as we propose (UKP*), the network scalability is enhanced.

5.2.2 Key ring size at equal network size

In this subsection, we compare the required key ring size when using the unital-based, the SBIBD-KP and the Trade- KP schemes at equal network size. We compute for each network size the design order allowing to achieve the desired scalability and we deduce then the key ring size, the obtained results are reported in Figure 5. The figure shows that at equal network size, the NU-KP scheme allows to reduce the key ring size and then the storage overhead. Indeed the enhancement factor over the SBIBD-KP scheme reaches 20. When using the t-UKP schemes, the results show that the higher t is, the higher required key ring size is. However, this value remains significantly lower than the required key ring size of the SBIBD-KP and the Trade-KP schemes. Moreover, we can see clearly in the figure, that at equal network size, the UKP* scheme provides very good key ring size compared the SBIBD-KP and the Trade-KP schemes. For instance, the key ring size may be reduced over a factor greater than two when using the UKP* compared to the SBIBD-KP scheme.

5.2.3 Energy consumption at equal network size

In this subsection, we compare the energy consumption induced by the direct secure link establishment phase. Since each node broadcasts its list of key identifiers to its neighbors, the energy consumption can be computed as :

$$E = Etx \cdot k \cdot log2(|S|) + \eta \cdot Erx \cdot k \cdot log2(|S|)$$

where Etx (resp. Erx) is the average energy consumed by the transmission (resp. reception) of one bit, k is the key ring size, η is the average number of neighbors and $log2(|S|)$ represents the size of a key identifier in bits that we round up to the nearest byte size. We compare the energy consumption of our solutions against SBIBD-KP and Trade-KP. The results plotted in equal network size, the NU-KP scheme consumes very small amount of energy to exchange the low.

5.2.4Network connectivity at equal key ring size

The key sharing probability when using the unital based schemes (NU-KP, t-UKP and UKP*). The figure shows that the NU-KP scheme provides a bad direct secure connectivity coverage which decreases significantly when the key ring size increases. Indeed, the key sharing probability is low and tends to $O(1k)$ as k tends to infinity. Otherwise, the obtained results show that the higher t is, the better the direct secure connectivity coverage is. Indeed, loading nodes with many blocks from unital design allows to increase significantly the key sharing probability. The figure shows moreover that the UKP* scheme gives very good connectivity results. For instance, the direct secure connectivity coverage remains between 0.82 and 0.66 when the key ring size is between 10 and 150. As the key ring size is high, the direct secure connectivity of UKP* approaches $1 - e{-}1 \approx 0.632$, which we proved to be an approximate lower bound.

5.2.5 Numerical results

We provide in table IV numerical results comparing network scalability, direct secure connectivity coverage, and average secure path length of the three schemes (SBIBD-KP, Trade-KP and UKP*) at equal key ring size. We notice that we provide the average network scalability (number of nodes) when using UKP* scheme. On the other hand, we compute the average secure path length based on simulations. We refer in these simulations to the results given in [23] in order to construct a grid deployment model which ensures the network physical connectivity and coverage. Numerical results show that the unital-based key pre-distribution scheme UKP* increases the network scalability over the SBIBD-KP and the Trade-KP scheme while maintaining high secure connectivity coverage. For instance, the network maximum size is increased by a factor of 3 and 4.8 when the key ring size is equal to 68 and 140 respectively compared to the SBIBD-KP scheme. In addition, we maintain a high connectivity over 0.63 which ensures a low average secure path length which does not exceed 1.37.

6. CONCLUSION

In this proposed work, a scalable key management scheme which ensures a good secure coverage of large scale WSN with a low key storage overhead and a good network esiliency. The make use of the unital design theory, that a basic mapping from unitals to key pre-distribution allows to achieve high network scalability while giving alow direct secure connectivity coverage. The proposed then an efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. It discuss the solution parameter and the propose adequate values giving a very good trade-off between network scalability and secure connectivity. The conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

REFERENCES

[1] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh-“ A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks”- IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013.

[2] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” *IEEE Commun. Surv. Tuts.*, vol. 10, no. 1–4, pp. 6–28, 2008.

[3] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. 2002 ACM CCS*, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *IEEE SP*, pp. 197–213, 2003.

[5] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, “A key management scheme for wireless sensor networks using dep loyent knledge,” in *Proc. 2004 IEEE INFOCOM*, pp 586–597.

[6] C. Castelluccia and A. Spognardi, “A robust key pre-distribution protocol for multi-phase wireless sensor networks,” in *Proc. 2007 IEEE Securecom*, pp. 351–360.

[7] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in *Proc. 2003 ACM CCS*, pp. 52–61.

[8] Z. Yu and Y. Guan, “A robust group-based key management scheme for wireless sensor networks,” in *Proc. 2005 IEEE WCNC*, pp. 1915–1920.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, “Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs,” in *Proc. 2011 IEEE INFOCOM*, pp. 326–330.

[10] S. Zhu, S. Setia, and S. Jajodia, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” in *Proc. 2003 ACM CCS*, pp. 62–72.

[11] S. A. C¸ amtepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks,” *IEEE/ACM Trans. Netw.*, vol. 15, pp. 346–358, 2007.

[12] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, “Spins:security protocols for sensor netowrks,” in *Proc. 2001 ACM MOBICOM*, pp. 189–199.

[13] B. Maala, Y. Challal, and A. Bouabdallah, “Hero: hierarchcal key management protocol for heterogeneous WSN,” in *Proc. 2008 IFIP WSAN*, pp. 125–136.

[14] W. Bechkit, Y. Challal, and A. Bouabdallah, “A new scalable key predistribution scheme for WSN,” in *Proc. 2012 IEEE ICCCN*, pp. 1–7.

[15] J. Zhang and V. Varadharajan, “Wireless sensor network key management survey and taxonomy,” *J. Netw. Comput. Appl.*, vol. 33, no. 2, pp. 63–75, 2010.

[16] S. A. C¸ amtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey,” Technical Report TR-05-07, Mar. 2005.