ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Highly Predictable Key Pre-Distribution Scheme for Wireless Sensor Networks

Haitham Ali Hussain
Master of Science (Information System),
Osmania University,
Basheer Bagh, Hyderabad.

T. Ramdas Naik
Assistant Professor, Computer Science (PG)
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

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 Predictability. Indeed, the protocol should support a large number of nodes to enable a large scale deployment of the network.

In this paper, we propose a new Predictable key management scheme for WSNs which provides a good secure connectivity coverage. For this purpose, we make use of the unital design theory. We show that the basic mapping from unitals to key pre-distribution allows us to achieve high network Predictability.

Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, we propose an enhanced unital-based key pre-distribution scheme providing high network Predictability and good key sharing probability approximately lower bounded by 1 – e 0.632.

We conduct approximate analysis and simulations and compare our solution to those of existing methods for different criteria such as storage overhead, network Predictability, network connectivity, average secure path length and network resiliency.

Our results show that the proposed approach enhances the network Predictability 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.

INTRODUCTION:
DEFINITION OF WSNs:

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

What are Wireless Sensor Networks and How It Works ?

In computer networking there is a great value of wireless networking because it has no difficult installation, no more expenditure and has lot of way to save money band time. In the field of wireless networking there is another form of networking which is called as wireless sensor network. A type of wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless sensor networking. Basically wireless sensor networking is used for monitoring the physical conditions such as weather conditions, regularity of temperature, different kinds of vibrations and also deals in the field of technology related to sound .

LITERATURE SURVEY:

The authors present a communication architecture for sensor networks and proceed to survey the current research pertaining to all layers of the protocol stack: Physical, Data Link, Network, Transport and Application layers. A sensor network is denied as being composed of a large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes collects data and its purpose is to route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user.The authors point out that none of the studies surveyed has a fully integrated view of all the factors driving the design of sensor networks and proceeds to present its own communication architecture and design factors to be used as a guideline and as a tool to compare various protocols. After surveying the literature, this is our impression as well and we include it in the open research issues that can be explored for future work.

SECURING WSNs: A SURVEY
AUTHORS: Y. Zhou, Y. Fang, and Y. Zhang

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, we 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.

A KEY-MANAGEMENT SCHEME FOR DISTRIBUTED SENSOR NETWORKS
AUTHORS: L. Eschenauer and V. D. Gligor

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, sensor capture detection, key revocation and sensor disabling. In this paper, we present a key-management scheme designed to satisfy both operational and security requirements of DSNs.

RANDOM KEY PRE-DISTRIBUTION SCHEMES FOR SENSOR NETWORKS
AUTHORS: H. Chan, A. Perrig, and D. Song

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 unlike liness 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-pair wise 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.

A ROBUST KEY PRE-DISTRIBUTION PROTOCOL FOR MULTI- WSNs
AUTHORS: C. Castelluccia and A. Spognardi

Wireless sensor networks are usually deployed to operate for a long period of time. Because nodes are battery-operated, they eventually run out of power and new nodes need to be periodically deployed to assure network connectivity. This type of networks is referred to as Multi-phase WSN in the literature [1]. Current key pre-distribution schemes, such as [2] and [3], are not adapted to multi-stage WSN. With these schemes, the security of the WSN degrades with time, since the proportion of corrupted links gradually increases. In this paper, we propose a new pre-distribution scheme adapted to multi-phase WSN.

In the proposed scheme, the pre-distributed keys have limited lifetimes and are refreshed periodically. As a result, a network that is temporarily attacked (i.e. the attacker is active only during a limited amount of time) automatically self-heals, i.e. recovers its initial state when the attack stops. In contrast, with existing schemes, an attacker that corrupts a certain amount of nodes compromises a given fraction of the total number of secure channels. This ratio remains constant until the end of the network, even if the attacker stops its action.

Furthermore, with our scheme, a network that is constantly attacked (i.e. the attacker regularly corrupts nodes of the network, without stopping) is much less impacted than a network that uses existing key pre-distribution protocols. With these schemes, the number of compromised links constantly increases until all the links are compromised. With our proposal, the proportion of compromised links is limited and constant.

PROBLEM STATEMENT:

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. The establishment of secure links between nodes is then a challenging problem 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 neighbouring nodes, that is why most existing solutions are based on key pre-distribution.

DRAW BACKS:

A host of research work dealt with symmetric key predistribution issue for WSNs and many solutions have been proposed In the existing system many disadvantages occur: the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

PROBLEM DEFINITION:

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

ADVANTAGES:

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 unital based 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.

IMPLEMENTATION:

Implementation is the carrying out, execution, or practice of a plan, a method, or any design for doing something. As such, implementation is the action that must follow any preliminary thinking in order for something to actually happen. In an information technology context, implementation encompasses all the processes involved in getting new software or hardware operating properly in its environment, including installation, configuration, running, testing, and making necessary changes. The word deployment is sometimes used to mean the same thing.

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.

CONCLUSION:

We proposed, in this work, a Predictable key management scheme which ensures a good secure coverage of large Predict WSN with a low key storage overhead and a good network resiliency. We make use of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows achieving high network scalability while giving a low direct secure connectivity coverage. We proposed then an efficient Predictable unital-based key pre-distribution scheme providing high network Predictability and good secure connectivity coverage.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We discuss the solution parameter and we propose adequate values giving a very good trade-off between network Predictability and secure connectivity. We 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] 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.

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

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

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. 2004 IEEE INFOCOM, pp. 586–597.

[5] C. Castelluccia and A. Spognardi, "A robust key predistribution protocol for multi-phase wireless sensor networks," in Proc. 2007 IEEE Securecom, pp. 351–360.

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

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

[8] 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.

[9] 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.

[10] 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.

AUTHORS BIOGRAPHY:

Haitham Ali Hussain, pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.

T. Ramdas Naik, Assistant Professor Dept, Computer Science (PG), Qualifications : B.E, MCA,M.Tech,(Ph.D) Nizam College (Autonomous),O.U, Basheer Bagh, Hyderabad, India.