April 2012

SECURITY ARCHITECTURE FOR REAL- WORLD APPLICATIONS OF WIRELESS SENSOR NETWORK

SHUBHI PRIYA

Department of Computer Science & Engineering , REVA ITM , Bangalore, spriya@gmail.com

SONALI SINGHA

Department of Computer Science & Engineering , REVA ITM , Bangalore, ssingha@gmail.com

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

PRIYA, SHUBHI and SINGHA, SONALI (2012) "SECURITY ARCHITECTURE FOR REAL- WORLD APPLICATIONS OF WIRELESS SENSOR NETWORK," *International Journal of Smart Sensor and Adhoc Network*: Vol. 2 : Iss. 3 , Article 7.

DOI: 10.47893/IJSSAN.2013.1160

Available at: <https://www.interscience.in/ijssan/vol2/iss3/7>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

A SECURITY ARCHITECTURE FOR REAL- WORLD APPLICATIONS OF WIRELESS SENSOR NETWORK

SHUBHI PRIYA¹, SONALI SINGHA², RASHIQUE JAMIL³, SHANTALA DEVI PATIL⁴
& VIJAYAKUMAR B P⁵

^{1,2,3,4}Department of Computer Science & Engineering , REVA ITM , Bangalore

⁵ Department of Computer Science & Engineering , MSRIT , Bangalore

Abstract: With the recent capability of being applicable in enormous fields, the Wireless Sensor Networks (WSN) have drawn attention of researchers and industries in diverse areas. Being deployed in areas that are hostile, WSN pose lots of difficulties and challenges to the research fraternity. In this paper, we discuss a generalized security framework for real world application of WSN. In particular we have considered the scenario of civil engineering field, a road tunnel. The proposed work mainly focus on security model for self adaptive lighting Model for road tunnel in WSN, and hence called Smart tunnel which provide the safety of the tunnels.

INTRODUCTION

Security is of a paramount importance for the deployment of WSN applications in a real environment. Due to the limited computation and communication capabilities offered by sensors, introducing security means to further reduce those resources for the application level. Therefore, the use of security primitives in WSNs requires to balance the needs for an adequate level of security while limiting the impact on resources. However, most of the security approaches for WSNs presented in literature are developed as stand-alone mechanisms that do not take into account the stringent requirements of realworld applications and deployments. For instance, TinySec [1] was one of the first work that addresses the security concern in WSNs. TinySec provides a fully implemented architecture for link-layer security in WSNs based on well-known cryptographic primitives. Another important aspect of TinySec is that its security properties exploit the limitations that are intrinsic of WSNs. For instance, WSNs have limited bandwidth. Therefore, it becomes possible to relax certain security properties and still guarantee adequate protection to specific attacks. Although TinySec provides a usable approach for WSN applications, pragmatic aspects that need to be addressed before a real deployment are left undefined. One of such aspects is key management.

The authors state that several options are available but not a single one is integrated with their architecture. Basically, it is left to the application developers to implement which key distribution mechanism is the best match for the characteristics of their applications. We believe that key distribution is an important aspect of a security architecture that constrains the integration with the application level. Therefore, key management must be concretely addressed before a seamless integration can be achieved.

Considering one of the real world scenario, a road Tunnel, an underground passageway completely enclosed except openings for ingress and egress. The operation of the tunnels is critical as it affects the safety of the drivers and also it involves the expenditure of energy for proper lighting. Studies have revealed some of the worst accidents that occurred in tunnels due to the lack of proper lighting and safety measures. Major accidents include especially from vehicle fires when combustion gases can asphyxiate users, as happened at the Gotthard Road Tunnel in Switzerland in 2001. One of the worst railway disasters ever, the Balvano train disaster, was caused by a train stalling in the Armi tunnel in Italy in 1944, killing 426 passengers.

Hence to avoid such accidents a self-adaptive lighting model inside the tunnel is required, which should be secure from attacks that are both physical and logical.

In section 1, we discuss with the deployment of the sensor nodes in the real world application, a road tunnel. Section 2, describes the security threats and the security requirements with respect to the tunnel application. The proposed generic Security architecture for a real world application using Self Adaptive Lighting Model to overcome these threats to provide security is discussed in section 3. Summary and conclusions are briefed in section 4.

1. Deployment of Sensor in Real world Application Scenario: Smart Tunnel

WSN is a collection of nodes with sensing capabilities and they have the ability to self organize. The deployment of the sensor nodes can be manual so that can get precise location information also is flexible and convenient. In this work we have considered a real world scenario a road tunnel as shown in figure 1, manual deployment of the sensor

nodes is best suited, as the sensor nodes are to be placed along the sides of the inner tunnel.

Figure 1: Smart Tunnel Scenario

In fact, each application based on WSN sensing technology has its own specific requirements which are derived from both the WSN setting specific to the application itself (nodes hardware, placement, access, just to mention a few) as well as from the overall requirements of the application where the information gathered through the nodes are collected. In this tunnel scenario the deployed sensors sense the light in the tunnel and gather the sensed information from all the nodes and forward it to the Base station, based on the light inside the tunnel the Base Station tunes the lighting system through the control room to reduce the energy consumption hence called as SELF-ADAPTIVE or SMART TUNNEL.

2. Security Threats and Security Requirements

By envisaging the tunnel scenario threats/attacks are possible, hence protecting the system from such threats is very important. The threats could be passive or active. Passive threats include listening to the communication and traffic analysis whereas, Active threats include reply attack and node compromise. To overcome these threats/attacks data integrity, confidentiality and authentication is required and to cater to these requirements a key management.

3. Proposed Generic Security Architecture for a Real World Application using Self Adaptive Lighting Model

The generic system Architecture for real world applications in WSN for providing security to road tunnels is as shown in as shown in the figure 2.

Figure 2. Proposed Security Architecture, Self Adaptive Lighting for Smart Tunnel

The different modules of the self-adaptive model are i: Node Deployment ii: Key Management iii: Data Aggregation iv: Data Processing. The function of the Node Deployment module is to manually deploy the sensor nodes along the inner perimeter of the tunnel. The second module is the key management module, the function is to generate and exchange the keys among the nodes so that the system could be secured which is discussed in detail in the next section. The third module of the system design is Data Aggregation Module which is responsible for the exchange of the sensed data between the nodes and the base station. The last module is the data processing that is received at the Base station and forwarded to the control room.

3.1 Key Management for Smart Tunnels

For existing attacks, many wireless sensor network key management scheme and authentication methods have been proposed. Schnauzer L. et al[2] proposed random key pre- distribution management scheme, and many scholars put forward a number of programs and protocols on this basis, such as the q-Composite Random Key Pre-distribution scheme and symmetric polynomial random key pre-distribution management scheme. For cluster-type network, some scholars have proposed a low-power key management scheme [5], lightweight key management scheme, key pre-distribution scheme based on cluster and key pre-distribution scheme based on ECC. Aiming at the limitations of existing scheme, the paper provides a key management scheme based on one-way Hash function and the symmetric key scheme. The analysis show that the proposed scheme can effectively weaken the threat of node capture, be resilience against node replication or node forgery. Besides of good security properties, the scheme promises good node addition or network extension ability.

Security in WSN can be achieved by proper Key management techniques. In general Key management has various phases such as i: key generation ii: pre-deployment iii: registration iv: post –deployment as discussed below.

3.2 Key Generation Phase: In this phase the different keys require are identified, the nodes use symmetric keys to communicate with the base station. Base station has pair of keys (public key and the private key) At first keys are generated using one-way hash functions. One-way hash function takes a binary string of arbitrary length as input, and outputs a binary string of fixed length. It is considered to have the following prerequisite properties: (1)Pre-image resistant: Given the output y, it should be hard to find any x, such that $y = \text{Hash}(x)$. (2)Collision resistant: It should be hard to find any x_1 and x_2 , such that $\text{Hash}(x_1) = \text{Hash}(x_2)$. The base station selects a random seed value say X_0 , the key for can be obtained by hashing this seed value as $\text{Hash}(X_0) \rightarrow X_1$ key. Then using this X_1 as the nest seed we get the second key as $\text{Hash}(X_1) \rightarrow X_2$ and so on for N keys where N is the number of Sensor nodes in the network. The keys generated by the station are stored in a key table, each of the key generated is unique and each node will be assigned a key from this table.

Pre-Deployment Phase:

In this phase the node placed with a secret key and the public key of the base station is deployed manually around the inner perimeter of the tunnel.

Registration Phase:

Each of the nodes deployed , will register themselves with the base station by sending an message which consists of NodeID,SecretKey encrypted using the Base Station Public key $\text{Message1} = \text{EpubBS}(\text{NodeID}, \text{Secret Key})$, the base station receives this message and decrypts it with its public key to obtain the identity of the node registering to the network. The base station forms a table that contains the nodeID and the Secretkey which will be used for further communication. All the nodes deployed register in the same manner with the base station.

POST-DEPLOYMENT PHASE:

Once the keys are deployed and the nodes registered the data sensing exchange begins.

3.3. Data Aggregation Phase:

The third module of the system design is Data Aggregation Module which is responsible for the exchange of the sensed data between the nodes and the base station. The exchange takes place as follows,

1: Data is sensed by the sensor(ie the intensity of the light in the tunnel)

2: The data then encrypted with the secret key possessed by the node

$\text{Message2} = \text{EsecretKey}(\text{data})$

$\text{Message3} = \text{EpubBS}(\text{Message2}, \text{NodeID})$

3: The message3 is then sent to the Base station

4: Base Station on receiving this Message will perform the decryption to obtain the message2 and the NodeID

5: The base station then uses the NodeID and checks the table to obtain the key corresponding to the node and decrypts to obtain the data . In this way data is received from the sensors and the value of the data is aggregated based on the number of messages received

3.4. Data Processing Phase:

In this module the data obtained by the base station is given to the control room, where the data is inferred and based on the inference the lighting of the tunnel is controlled.

4. RESULTS AND CONCLUSIONS

COMPARISON OF SMART TUNNEL WITH NORMAL TUNNEL LIGHTING

Figure 3: Comparisons of Smart Tunnel with Normal Tunnel

The key management scheme discussed provides security among the nodes and also between the nodes and base station. All nodes authenticate by registration process with the base station. By using encryption we provide confidentiality. The above graph shows that the smart tunnel is energy efficient and also secure.

REFERENCES

- [1] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesc language: A holistic approach to networked embedded systems." in *Proc. of ACM SIGPLAN 2003 conference on Programming language design and implementation*, S.Diego, California, USA, 2003.
- [2] "Tinykey project web-page." [Online]. Available: <http://gforge.create.net.org/gf/project/tinykey>
- [3] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher blockchaining message authentication code." *Journal of Computer and System Sciences*, vol. 61(3), pp. 362–399, December 2000.
- [4] E. Brickell, D. Denning, S. Kent, D. Mahler, and W. Tuchman, "Skipjack review." *Interim report*, 1993.
- [5] A. Francillon and C. Castelluccia, "TinyRNG: A Cryptographic Random Number Generator for Wireless Sensors Network Nodes." in *WiOpt. 5th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, 2007.
- [6] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-lowpower wireless research." in *Proc. of 4th International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, UCLA, Los Angeles, California, USA, April 2005.
- [7] P. Costa, L. Mottola, A. Murphy, and G. Picco, "TeenyLIME: Transiently Shared Tuple Space Middleware for Wireless Sensor Networks." in *Proc. of 1st Int. Workshop on Middleware for Sensor Networks (MidSens)*, 2006.
- [8] "TinyOS. TEP 105 - Low Power Listening." [Online]. Available: <http://www.tinyos.net>
- [9] C. E. Shannon, "A mathematical theory of communication." *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, July, October 1948.