International Journal of Research in Social Sciences
Vol. 9, Issue 4, April - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

PERFORMANCE AND STUDY OF WIRELESS MULTIMEDIA SENSOR NETWORKS SECURITY ISSUES

Vinam Tomar[1], Dr. Rajiv Kumar[2]
Department of Computer Science
[1,2]Shri Venkateshwara University, Gajraula (Uttar Pradesh)

Abstract-Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Wireless Sensor Networks (WSNs) are the collectors of information from the physical world in the form of sensed data according to the requirement like temperature, pressure, humidity, level, movement etc.This data is available to the sink through gateway. Sensors are deployed in extensive numbers and on account of its wireless nature; it is easily works in any type of environment. Although sensor nodes are deployed in a random manner still it's important to deploy them carefully. Deploying few nodes may raise the issue of coverage and deploying too many nodes may result in an inefficient network because of more collision and interference. Wireless Sensor Networks (WSNs) need effective security mechanisms because these networks deployed in hostel unattended environments. Due to inherent limitations in wireless sensor networks, security is a crucial issue. While research in WSN security is progressing at tremendous pace, no comprehensive document lists the security issues and the threat models which pose unique threats to the wireless sensor networks.This article investigates and assess energy efficient multimedia group for wireless sensor network.

Keywords: Wireless Sensor Networks, Algorithms, Programming Models, Data Management, Multimedia

1. Introduction

A WSN is a sensor node with a limited capacity for processing, limited storage and limited communications bandwidth, limited resources and hardware size. There are currently so many kinds of sensor nodes on different platforms. The protection of sensor nodes in real life also matters with the hardware. Some criteria for safe communication have to be met by the sensor network. Availability, confidentiality, honesty and

authentication are general requirements of WSN protection. Source localization, self-organization and data freshness are other criteria called secondary requirements. These requirements protect data transmitted over the sensor network against attacks.

- **Data Confidently**

In sensor network, data flows from many intermediate nodes and chance of data leak is more. To provide the data confidentiality, an encrypted data is used so that only recipient decrypts the data to its original form.

- **Data Integrity**

Data received by the receiver should not be altered or modified is Data Integrity. Original data is changed by intruder or due to harsh environment. The intruder may change the data according to its need and sends this new data to the receiver

Data Authentication
It is the procedure of confirmation that the communicating node is the one that it claims to be. It is important for receiver node to do verification that the data is received from an authenticate node.

- **Data availability:** Data Availability means that the services are available all the time even in case of some attacks such as Denial of service.

- **Source localization:** For data transmission some applications use location information of the sink node. It is important to give security to the location information. No secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

- **Self-organization:** In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self-organizing and self-healing properties. This is a great challenge for security in WSN.

- **Data freshness:** Data freshness means that each message transmitted over the channel is new and fresh. It guarantees that the old messages cannot be replayed

by any node. This can be solved by adding some time related counter to check the freshness of the data.

2. Typical Security Treats and Defense Techniques in Wireless Sensor Networks

By default, connectivity over wireless networks is unreliable and easily vulnerable to different kinds of treatments. There are a vast number of sensor nodes in a large-scale sensor network and they can be spread over a large area. With limited communication and computing capabilities, typical sensor nodes are small. Several primary types of treatments are interpreted by these tiny sensor nodes. Monitoring and shielding each individual sensor from physical or logical attack is impractical for a large-scale sensor network. Sensor network threats can be categorized into physical, connection (MAC), network, transportation, and application layer attacks.

Treats may also be categorized on the basis of the potential attacker's capacity, such as sensor level and laptop level. A strong adversary at the laptop level can do much more damage to a network than a malicious sensor node, as it has much better power supply and greater processing and networking capabilities than a sensor node. Treats can also be divided into treats that are outside and inside. In sensor networks, an outside attacker does not have access to most cryptographic materials, while an inside attacker may have partial key materials and the trust of other sensor nodes. Attacks inside are much more difficult to detect and protect against. The three simplest main models used to compare the various relationships between the security and operational requirements of the WSN are:

- Network keying
- Pair-wise keying, and
- Group keying

Over the other two systems, the network keying model has inherent advantages. It is straightforward, easy to handle, and requires very few resources. Network keying also

helps nodes to quickly communicate as neighboring nodes can read and interpret data from each other, fulfilling the criteria for self-organization and accessibility. In terms of scalability and stability, it is also excellent since there is only one key for the whole network, and with the addition of nodes, it does not shift. An undesirable downside to robustness, however, remains. Suppose one node is compromised, and the key is revealed in the network. With this key, an opponent may eavesdrop on all network messages and even insert forged messages into the network, potentially undermining the network's proper activity. At the other extreme, in each node, the pair-wise key model uses the N-1 key, where N is the network size.

Although this model offers the ultimate in robustness against node capture, no other node is not compromised by the compromise of one node. Since the storage cost increases rapidly with network size, it fails to fulfill the scalability criterion. In the case of several thousand nodes, it becomes unmanageable to hold the number of keys each node must maintain. Consider the per node storage of N-1 keys. The network's total number of distinguishable keys is N(N-1)/2, which rises at a rate of N2. When N is a large value, this is not maintainable. Another problem with the model of pair-wise keying is that it is difficult to add new nodes to the network, impacting the need for versatility. Any node must obtain a new key to communicate with it when a new node is added. This is a resource-intensive method that, as compared to the simple preloading of a network-wide key as in the previous model, uses far more precious resources.

In the same way, key revocation and key refreshing suffer from the same problem of scalability. In addition, as nodes do not passively track event signals, the accessibility requirement is in jeopardy. Finally, self-organization comes into question in the case of pairwise key distribution systems, since they resolve the scalability issue by reducing the number of mutual keys, resulting in certain nodes being unable to connect with others and undermining the network's self-healing and self-organizing skills. The group keying framework incorporates the characteristics of both network and pair-wise keying systems. Communications are conducted using a single, shared key similar to network keying within a group of nodes forming a cluster. Communications between groups, however,

use a separate key between each pair of groups in a way similar to the scheme of pair-wise keying.

3. Security in Group Communications Over WSNs

Safe community communications over WSNs provide security protection. For large-scale distributed sensor networks, a key management protocol called a localized encryption and authentication protocol (LEAP) where each sensor node with its one-hop neighbor will generate pair-wise keys. In order to reach cluster heads, multi-hop pair-wise key may be required and it can be done by each node generating a secret key and finding m intermediate nodes. The protocol is built on the basis of two observations: different packet types exchanged between sensor nodes require various security services, and a single key management system may not be sufficient for different security requirements. In order to encrypt communications, four types of keys for fundamental security services may be used.

These four key types include a pair-wise key used between a sensor node and the base station, a pair-wise key used between a pair of two sensor nodes, a shared cluster key used between all sensor nodes in the same cluster, and a community key used between all sensor nodes. Security services can be offered that can prevent many attacks. Authenticating one-hop broadcast communications between nodes with one-way key chains, for example, will reduce the impersonation attack, while using a time stamp to expire keys to avoid catching nodes and sybil attacks. The ability to upgrade software following implementation is a critical problem in the successful deployment of these networks.

The software related to WSNs contains all application-specific tasks and middleware functions to construct and manage the network, such as routing, node search, service discovery, and self-localization. There are a number of reasons why the software in a WSN would need to be modified. Four types of software updates for defensible systems are defined by the Software Engineering Institute (SEI) at Carnegie Mellon University to help provide insight into these reasons: maintenance releases, minor releases, major releases (technology refresh) and technology insertion. It is possible that embedded wireless sensor systems programmed by specialists would experience higher than usual maintenance levels. Minor releases can be used to enhance the efficiency and collection of data.

Since the needs of WSNs are likely to evolve dynamically over time, it is possible to anticipate significant releases in response. Finally, due to active research on WSNs and

related technologies and the associated development of new technology algorithms and protocols, the implementation of software updates would be an important driver. Wireless sensor nodes are distinguished by extremely limited resources and implementation on a wide scale. It can be hard to find or inaccessible to access these nodes in the field to conduct software upgrades, or the size of the deployment can prevent individual access. Remote update presents its own issues.

4. Wireless Multimedia Sensor Networks Applications and Security Challenges

Wireless multimedia sensor networks promote the emergence of low-cost and mature innovations in wireless networking, visual sensor applications, and digital signal processing (WMSNs). WMSN interconnects autonomous devices for capturing and processing video and audio sensory information, much like sensor networks that respond to sensory information such as humidity and temperature. New applications like multimedia surveillance, traffic enforcement and control systems, advanced delivery of health care, systemic health monitoring, and control of industrial processes will be allowed by WMSNs. Because of WMSNs, there are some new features that stem from the fact that some of the sensor nodes would have video cameras and greater computing capabilities. As a result, the WMSNs offer new protections as well as new possibilities for challenges.

This paper addresses the implementation and security problems of WMSNs. The development of a wireless multimedia sensor network has been encouraged by the availability of multimedia devices such as small microphones and low-cost complementary metal oxide semiconductors (CMOS) (WMSN). Multimedia content such as scalar data, streaming audio and video can be captured from the environment by these multimedia devices. A WMSN will thus be able to send and receive multimedia content, such as data monitoring, image, voice, and video streaming. Because of the ability to retrieve multimedia data, the WMSN will also be able to store, process, compare and fuse multimedia information from various sources in real time. Therefore, WMSNs consist of multiple types of multimedia sensors that use wireless channels to share sensed multimedia data with sink. Not only will WMSNs boost existing sensor applications such as tracking and monitoring of the environment, but they will also enable many new applications.

They range, for example, from telemedicine support systems to modern military ones. Data collected from the environment is not only a scalar nature in WMSNs, obtained from different internal sensors such as temperature, light, humidity, pressure, and acoustic sensors, but also from multimedia data such as digital images, video, and audio.

International Journal of Research in Social Sciences
Vol. 9, Issue 4, April - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Therefore, in WMSN, the main sensor is the imager. The visual data that is treated imposes serious constraints on a network of sensors. A processing intensive and high bandwidth demanding activity is the compilation, processing, and visual data dissemination. WMSNs have some new features that stem from the fact that video cameras and higher computing capacities are available for some of the sensor nodes.

As a result, the WMSNs bring new challenges of protection as well as some new opportunities. In this segment, particularly in the multimedia sensor node, we discuss WMSN hardware components. It notes that multimedia sensor hardware for enabling hardware platforms has been split into two groups based on its resolution.

5. Conclusion

In WSN design, protection mechanisms can be important. Recent work has focused on creative mechanisms that, depending on the available resources of sensor networks, provide different levels of protection. For WSN applications, encryption is very important in this context, as these networks are highly vulnerable to security breaches because of their wireless and distributed existence. An significant method to ensure protection in networks with resource constraints is selective encryption of images.

As conventional encryption methods may be unfeasible for WISN due to high computational and communication overhead, the combination of encoding algorithms with cryptography may be a viable solution. Watermarking and safe image tracking authentication are also important concerns that have been discussed in this work. The analysis carried out has contributed significantly to wireless image sensor network investigations, potentially promoting important studies in the coming years.

The characteristic of a WMSN diverge consistently from traditional network paradigms, such as the internet and even from the WSNs. The most potential applications of WMSNs require the sensor networks paradigm to be rethought to provide mechanisms to delivery multimedia contents with the predetermined level of Quality of Service (QoS).

WMSNs will enable several new applications:

- **Surveillance:** WMSNs are used currently in surveillance which needs streaming multimedia content, advanced signal and high bandwidth. Such as Audio and video sensors will be used to complement and enhance existing surveillance systems against crime attack.

- **Traffic monitoring and Enforcement:** WMSNs are low cost, easy of deployment and ease for reconfiguring routes when deployment in the specific location such as in big cities of highways. They will be possible to monitor car traffic and to service that offer traffic routing advice to avoid congestion.

- **Personal and Health care:** WMSNs, incorporated with some telemedicine devices, can be used to remotely monitor the patient's body temperature, blood and breathing activity etc. They can be studied the behavior of elderly people as means to identify the causes of illnesses that affect them such as dementia.

- **Gaming:** WMSNs will find applications in the future prototypes that enhance the effect on the game player. Such as virtual reality games that assimilate touch and sight input, of user as part of the player response.

- **Environmental and industrial:** Array of video sensors are used by Oceanographer to determine the evolution of sandbars using image processing techniques and multimedia content such as imaging, temperature, or pressure can be used for time-critical industrial process control.

Sensor nodes in a wide, unattended area are often deployed. Without being detected, an attacker can compromise one or a number of sensor nodes. As a result, no solution for WMSNs is directly deployed. New approaches should therefore be established that leverage the characteristics of multimedia nodes.

Many papers describe the deployment of sensor nodes. For example, the design of multimedia sensor networks to support volcanic studies involves addressing the high data rates and high data fidelity and the sparse array with high spatial separation between nodes, but the protection of the sensor node deployment procedure for a wireless sensor network is not defined in this report.

It is intended to direct users to systematically complete the tasks of deployment research on optimized node placement in WSNs. Both are used only to deploy WSN and are not concerned with protecting the sensor node.

References

Jun Wu, Kaoru Ota, Mianxiong Dong, Chunxiao Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, Vol. 4, pp. 416–424, 2016.

2. Agnihotri, Ram Bhushan, Ajay Vikram Singh, and ShekharVerma. "Challenges in wireless sensor networks with different performance metrics in routing protocols." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1– 5. IEEE, 2015.

3. Goutam Mali, SudipMisra, "TRAST: Trust-Based Distributed Topology Management for Wireless Multimedia Sensor Networks", IEEE Transactions on Computers, Vol. 65, Issue: 6,pp. 1978–1991, 2015.

4. Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30–33.

5. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

6. Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003).vol.1, pp. 335–340.

7. Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41–50.

8. Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on physical layer", IEEE GLOBECOM 2003, Volume 3, 1–5 December, 2003, pp. 1226–1230.