Recouping the Modified Data in Intruder-Based Environment

Ambika Nagaraj, Dayananda Sagar College of Engineering, Bengaluru, India

ABSTRACT

Sensor networks are playing an important role in many applications. These networks mainly used as monitoring tool are deployed in harsh and unsupervised environment. Hence securing these nodes and the data which is being transmitted becomes a basic requirement. To adapt security to the network, the study uses cluster-based arrangement of nodes. The encryption key is generated based on location, which enhances security by incorporating authentication, reliability and confidentiality of data. The packets are being analysed for its fidelity by the nodes which fall in path of the base station. Compared to the previous contributions certain amount of energy is conserved. Addition to this procedure, the data can be retrieved if modified by the adversary. The scheme enhances the security against sinkhole, wormhole and Sybil attacks.

Keywords: Authentication, Confidentiality, Detection & Prevention Technique, Integrity, Mobile Agent, Reliable, Retrieving Data, Sensor Network

1. INTRODUCTION

New technologies are making a break through the previous ones reducing the human effort, amplifying speed of production and its productivity. Any technology is brought into reality to ease human effort and to provide better living style. The basic design of a sensor consists of transmitter, sensor and receiving components. Earlier these nodes were not used in some applications due to their limitations. Redefining the design made these devices usable in many applications discussed by many authors in their work (Pottie & Kaiser, 2000) (Chong & Kumar, 2003) (Hakala, Tikkakoski & Kivela, 2008) (Zhuang, Goh, & Zhang, 2007) (Gungor & Hancke, 2009), from simple to complex. Some of the applications where these sensors are one of the essential part includes military surveillance portrayed by the author in the work (Sang Hyuk Lee, DOI: 10.4018/IJERTCS.2014070102
Soobin Lee, Heecheol Song & Hwang Soo Lee, 2009), habitat monitoring discussed by authors (Alan, David & Joseph, 2002) (Robert, Eric, Joseph & Michael, year) (Naumowicz, Freeman, Kirk, Dean, Calsyn, Liers, Braendle, Guilford & Schiller, 2010), forest fire detection illustrated by the authors in their work (Hefeeda, Bagheri, Simon & Surrey, 2007) (Mal-Sarkar, Sikder & Konangi, 2010) etc.

These tiny devices is mentioned by the author (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002) are adding a better value to life by monitoring and tracking the object of interest. These nodes collaborate together to accomplish a defined task. The nodes can gather information without any human intervention and communicate to the required pre-defined destination. The adversary can take an advantage of this and access to the confidential data stored in the nodes. The intruders camouflage as a member of the cluster and falsify the visualization of the network. Hence these intruders have to be detected and detached from the network on time. To avail this facility, a better algorithm has to be devised.

The paper is modelled to enhance security to the data being transmitted. To do so, the proposed work uses static nodes to sense the environment. Mobile robots are utilized to provide the location details and they are involved in authenticating the cluster head. Four kinds of detectors are being positioned at different locations in the network to ensure reliability to the network. The proposed model provides integrity, reliability and confidentiality similar to the work proposed by other authors (Aysal & Barner, 2008) (Giruka, Singh, Royalty, Varanasi, 2008) (Kundur, Luh, Okorafor, Zourntos, 2008) (Wang, Attebury, Ramamurthy, 2006).

The contributions of the paper are as follows:

1. The proposed model guarantees the regeneration of the modified message transmitted by the nodes in the network. The recovery is $\geq 98\%$ to the transmitted message;
2. The work protects the network significantly against Sybil, Sinkhole and Wormhole attack;
3. The previous encryption key utilized is erased after its utilization. This provision provides backward secrecy to the network. The encryption key generated varies with time and data being sent. Hence the future encryption key can’t be predicted. This method provides forward secrecy to the system;
4. The paper conserves certain amount of energy by eliminating false data injection, utilizing multi-hop transmission and eliminating some part of communication.

The succeeding section provides a brief history of the work done before. Section 3 depicts notations used in the work. Segment 4 illustrates the assumptions made while designing the paper. Section 5 provides a detail description of the study. Section 6 justifies the work. Section 7 gives a detail report of the
Adoption of Model-Based Testing and Abstract Interpretation by a Railway Signalling Manufacturer
www.igi-global.com/article/adoption-model-based-testing-abstract/54248?camid=4v1a

A Survey of FPGA Dynamic Reconfiguration Design Methodology and Applications
www.igi-global.com/article/survey-fpga-dynamic-reconfiguration-design/66430?camid=4v1a