ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOG

# Performance Comparison Wireless Sensor Network Security Protocols : LLSP and Tiny SEC

**Yones Bazband*, Kamran, fahimi**
Islamic Azad University Khoramabad
bazvand438@gmail.com

## Abstract

Security protocols play an important role in the deployment of sensor networks in various environments However, many existing security protocols developed for WSNs are vulnerable to attacks in hostile environments. This paper reviews and compares the Delivery ratio and power consumption for two protocols LLSP and Tiny Sec in WSN to determine which protocol is suitable for each network and application type.

**Keywords**: Wireless Sensor Network, Security, LL

## Introduction

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. Each node consists of a microcontroller (performs tasks, processes data and control components), transceiver (combined functionality of transmitter and receiver), external memory[1]. Wireless sensor network (WSN) has momentous applications like remote environmental monitoring and target, these sensors are provided with wireless interface those wireless ports can combine a network by communicate to each other Sensor network one of the ad hoc mobile networks. Major parameters [2] for WSN security includes Key management, providing secrecy and authentication, ensure privacy, robustness against communication denial of service attack, secure routing, energy efficiency, and resilience to node capture.Two different protocols for Wireless Sensor Networks (WSN) are analyzed to study the most effective protocol taking into account limitation of energy and delivery ratio to guarantee along live time for sensor nodes battery and to ensure our network is working in critical applications.

## Related works

In wireless sensor networks there are several protocols, however this paper will focus on analysis of two security protocols. LEDS incorporate location aware key management framework where each key is bind with location information. Localization helps to isolate the impact for a compromised key. filtering in WSNs. In particular, it is designed to achieve the following goals:Provide end-to-end data condentiality and authenticity Achieve high-level of assurance on data availabilityThis approach helps to prevent master key disclosure using compromised nodes[3] SPINS is a protocol developed to solve the particularly difficult WSN problem of broadcast authentication. SPINS is built of two protocols called SNEP and µTesla.SNEP provides security between two nodes, while µTesla provides broadcast authentication using symmetric keys. [4] SNEP uses block ciphers to encrypt messages in Cipher Block Chaining (CBC) mode. µTesla provides broadcast authentication using a delay strategy. µTesla begins with the gateway generating a key chain by continuously applying a hash function and reversing the order of the keys. Each node entering into the network must be bootstrapped with a key in the keychain. The bootstrapped key is a commitment to the key chain because subsequent keys can be authenticated with repeated applications of the hash functions to return to the initial key value. The network is synchronized by intervals to which a new key is bound to. Packets send during an interval contain a MAC encrypted with the intervals key. After each interval, the gateway releases another key. A node can validate the key by applying the hash function to obtain the previous rounds key.µTesla does have its flaws. Because nodes must buffer data before keys are revealed, attackers can send random messages to overflow the nodes buffer. The receiving node is unable to determine which messages are from the gateway until the key is revealed.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

## LLSP protocol

LLSP security protocol guarantees message authentication, access control, message onfidentiality and replay protection. Data encryption is a method of achieving message confidentiality when transmitting data through an unsecured medium. For the LLSP security protocol, we propose the Advance Encryption Standard (AES) with cipher block chaining (CBC) mode of operation as the data encryption scheme To guarantee message authentication and access control,LLSP uses a message authentication code (MAC)[5]. Message authentication prevents unauthorized nodes from participating in the network and ensures received messages are not altered,thus inherently assuring the message contains no errors. A MAC is essentially a cryptographically secure checksum of a message. Computation of the MAC is based on a cryptographic hash function and a secret shared key between the sender and receiver. In a replay attack, an adversary eavesdrops between two authorized sensor nodes and replay the message to the receiver at a later time. Typically, a counter value is used to maintain record of the received messages from a node. If the authorized receiver has a record of the received message, it can detect a replayed message and reject it. But, if there is no record of the received message then the receiver will accept the message again, consequently increasing the energy consumption.

## Tiny SEC protocol

Tiny Sec protocols, the dominant traffic pattern in sensor networks is many-toone,with many sensor nodes communicating sensor readings or network events over a multihop topology to a central base station. However, neighboring nodes in sensor networks often witness the same or correlated environmental events, and if each node sends a packet to the base station in response, precious energy and bandwidth are wasted. To prune these redundant messages to reduce traffic and save energy, sensor networks use in-network processing such as aggregation and duplicate elimination [6]. Since in network processing requires intermediate nodes to access, modify, and suppress the contents of messages, it is unlikely we can use end-to-end security mechanisms between each sensor node and the base station to guarantee the authenticity,integrity, and confidentiality of these messages. With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. Single shared global cryptographic key, link layer encryption and integrity protection cryptography is based on a block cipher. TinySec is a research platform that is easily extensible and has been incorporated in to higher level protocols. TinySec includes a two byte counter to provide randomness in the IV. However, these two bytes are not used for replay protection. TinySec prevents Injection and alternation attack using MAC

## Implementation and network design

To evaluate the effectiveness and the efficiency of LLSP and LEDS wireless sensor network protocols, this paper design a network topology in addition to the sink node using NS2simulator.figure1

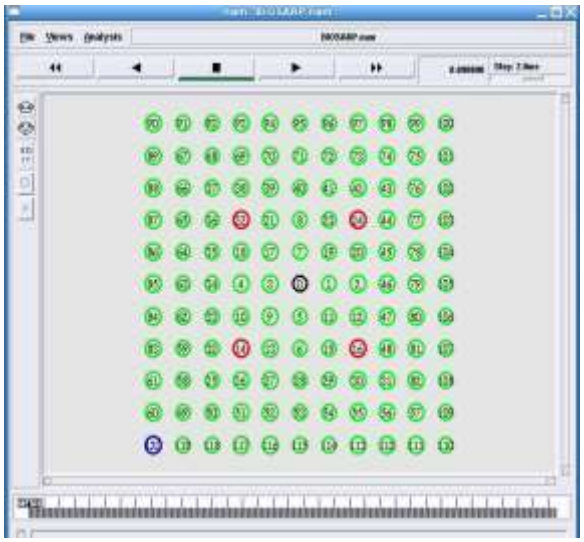

***Fig. 1. Network Simulation Grid***

## Compartion between llsp and tiny sec

**Delivery Ratio**

To evaluate the delivery ratio this project will use the network which showed in figure 1. The result show below in figure2 gained after run the NS-2 simulator with one source node and four malicious nodes to check the performance of LLSP and Tiny Sec due to our first parameter delivery ratio. Figure2 show that LLSP performance is good than Tiny Sec in case of using four malicious nodes attack implemented wireless sensor network.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

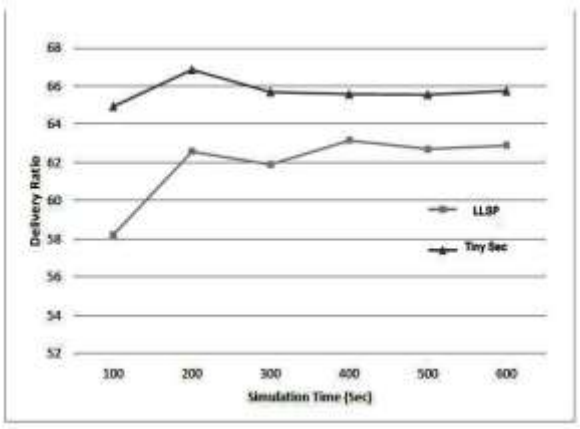


***Fig. 2. Delivery ratio comparisons LLSP V.S Tiny Sec***

## Power consumption

To evaluate the performance of consuming energy in implemented network of this work which showed in figure1The result show below in figure 4 gained after run the NS-2 simulator to second parameter power consumption. In Figure 3 shown that LLSP energy consumption is better than Tiny Sec. The result clearly show view the power consumption is increasing with increasing the simulation time for both LLSP and Tiny Sec protocols.

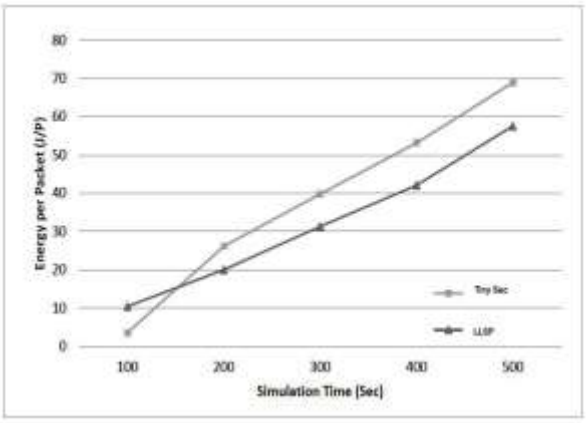


***Fig. 3. Delivery ratio comparisons LLSP V.S Tiny Sec***

## Conclusion

The results shown which LLSP protocol use In network processing applications Resource constraint environment Small sized network.

## *References*

[1] *Chien T.V., Chan H.N., Huu T.H. A Comparative Study on Operating System for Wireless Sensor Networks. Proceedings of 2011 International Conference on Advanced Computer Science and Information System (ICACSIS); Jakarta, Indonesia. 17–18 December 2011.*

[2] *Adrian Perrig and John Stankovic and and David Wagner.Security inWireless Sensor Networks. In Communicationof the ACM, volume 47, page 53, June 2004.*

[3] *Kui Ren andWenjing Lou and Yanchao Zhang. LEDS:Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. In Mobile Computing,IEEE Transactions, volume Voloume: 7, Issue: 5, page 585, May 2008.*

[4] *Taejoon Park and Kang G. Shin. LiSP: A Lightweight Security Protocol for Wireless Sensor Networks. In ACM Transaction, June 2004.*

[5] *Liu, Y., et al. (2007), 'A routing strategy based on ant algorithm for WSN', (5: IEEE), 685-89.6.*

[6] *Chris Karlof and Naveen Sastry and David Wagner.TinySec: A Link Layer Security Architecture forWireless Sensor Networks. In SenSys,ACM, November 2004.*

## Author Biblography

| | |
|---|---|
|  | **Uones bazvand**<br>Masters of Information Technology Engineering in Computer Networks Field<br>Email: bazvand438@gmail.com |
|  | **kamranfahimi**<br>Software Engineering in Computer Networks Field<br>Email: **kamranfahimi**22@yahoo.com |