I J C T A, 9(31), 2016, pp. 89-97 ISSN: 0974-5572

Efficient Secure Management Technique (ESMT) in Mobile Wireless Sensor Networks

R. Dharani* and M. V. Srinath**

ABSTRACT

Wireless Sensor Networks (WSNs) have enabled a wide spectrum of applications through networked low cost low power sensor nodes. Mobile Wireless Sensor Networks have all the nodes moving in the network and they are the most important in the current developing fields. One of the most vital challenges in this fast developing technology is the absence of routing enhancing protocols along with the improved security. Therefore, in this paper we propose a Efficient Secure Management Technique (ESMT) in Mobile Wireless Sensor Networks to give improved performance. The simulation analysis shows the improved performance of the proposed ESMT mechanism. Simulation scenarios are designed using the network simulator (NS-2).

Keywords: Wireless Sensor network, Efficiency, Routing algorithm, Security, Communication, Mobility.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have a wide range of applications through networked low cost low power sensor nodes. Examples include precision agriculture, habitat monitoring and forest fire detection. In these applications, the WSN will operate under few human interventions either because of the hostile environment or high management complexity for manual maintenance. Energy saving is of supreme importance in the design of sensor network protocols the reason being sensor nodes have limited battery life. The task of the sensor nodes is to sense the physical phenomena from their neighbor nodes and transfer the sensed data to the base stations. As the number of nodes is very large and sensor nodes have constraints including power, computation, communication and storage, multi-hop communication is preferred in WSN.

The major concern in today's wireless world is the lack of security. Security in WSN becomes crucial since the nodes after the deployment cannot be manually maintained. Due to its network of communication, this situation becomes a major issue in WSN. The authentication is provided to the data that can be sent or accessed by any node in the communication network. Preventing and gaining the information from the unauthorized users is considered to be a critical task. As new threats and attack models are proposed, several authentication mechanisms have been introduced in WSN security.

2. RELATED WORKS

A large number of existing algorithms are there for routing and security purpose, of which each of them has their own disadvantages.

User Authentication (UA) is an important issue in designing dependable and secure systems [1]. Consider a WSN is deployed in an intelligent building or a university campus to allow legitimate users to send queries and retrieve the respective result at any of the sensor nodes in the communication network. The

* Research Scholar, Department of Computer Science, S.T.E.T. Women's College, Mannargudi, India,*Email: dharaninagavalli@gmail.com*

** Director of Department of MCA, S.T.E.T. Women's College, Mannargudi, India.

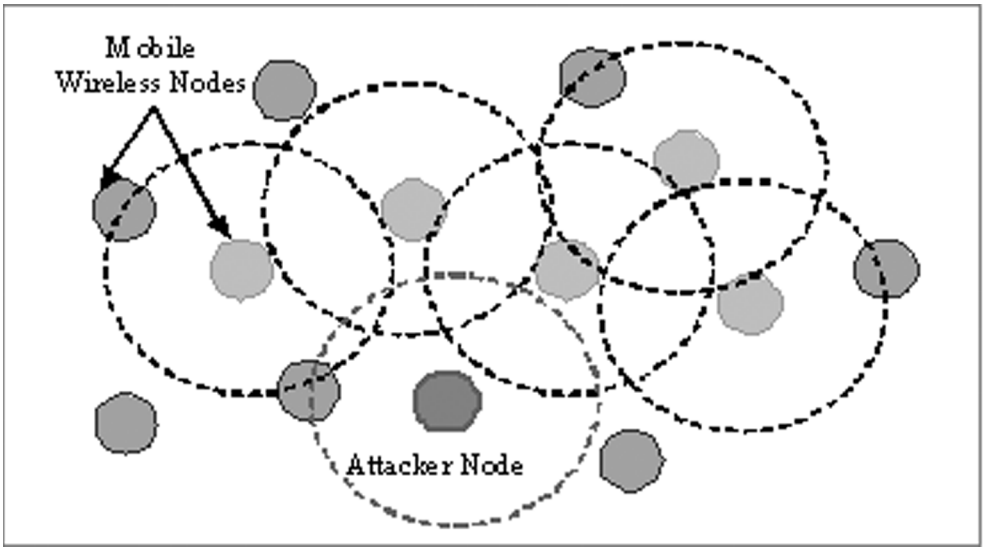

Figure 1: Mobile Wireless Sensor Network with an Attacker

system needs to provide a means of user authentication to verify if the user is valid. A dynamic strong-password based solution was designed to this access control problem and adapts it into a WSN environment. The designed strong password authentication approach imposes very light computational load and requires simple operations such as one-way hash function and exclusive-OR operations. Analysis on security and communication costs is presented to evaluate the effectiveness of this scheme.

Due to the critical resource constraints of wireless sensor nodes such as memory size, processing speed and energy supply, implementing security mechanisms, in particular key management schemes, is quite challenging. LPKM (Lightweight Polynomial-based Key Management Protocol), a key management scheme for distributed WSNs enables sensor nodes to establish different types of keys to bootstrap trust and secure one-to-one and one-to-many communications in a flexible, reliable and non-interactive way [2]. Also LPKM can effectively mitigate or thwart the most common attacks such as node clone attacks and node impersonation attacks to WSNs. In addition, LPKM can tolerate changes of network topology and incurs little computational and communication overhead.

A lightweight user authentication scheme was adapted to WSNs that provides mutual authentication and session-key agreement [3]. This scheme allows a user equipped with mobile device to authenticate him before gaining access to the WSN. The scheme is executed at two sides; the client which controls the user's mobile device and the server represented by the coordinator of the WSN. The security analysis of the scheme proves its resilience against classical attacks. The scheme is also implemented on real platform of sensor nodes. This implementation proves that this scheme is lightweight and rapid as it requires approximately only 1s to be fully executed.

SPINS has two secure building blocks namely SNEP and μTESLA. SNEP includes two-party data authentication, data confidentiality and evidence of data freshness.μTESLA provides authenticated broadcast for severely resource-constrained environments [4]. The SNEP and μTESLA protocols show that they are practical even on minimal hardware. The performance of the protocol suite matches the data rate. Additionally, the suite can be used for building higher level protocols in the communication newtwork.

LEAP+ (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks was designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the network neighborhood of the compromised node [5]. The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements and that a single keying mechanism is not suitable for meeting these

different security requirements. LEAP+ supports the establishment of four keys for each sensor node that includes an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes and a global key shared by all the nodes in the communication network. LEAP+ supports local source authentication without precluding in-network processing. LEAP+ was evaluated under various attack models and shown that LEAP+ was very effective in defending against many sophisticated attacks including node cloning attacks, HELLO flood attacks and wormhole attacks.

Elliptic curve cryptography over F2p for sensor networks was known based on the 8-bit, 7.3828-MHz MICA2 mote [6]. Although public-key infrastructure has been thought impractical, through analysis of the implementation for TinyOS of multiplication of points on elliptic curves, that public-key infrastructure is viable for TinySec keys' distribution, even on the MICA2. The public keys can be generated within seconds and that shared secrets can be distributed among nodes in a sensor network within the same, using just over one kilobyte of SRAM and certain kilobytes of ROM.

An efficient and scalable protocol was proposed to establish and update the authentication key in a dynamic WSN environment [7]. The protocol guarantees that two sensor nodes share at least one key with probability 1 with less memory and energy cost not causing considerable communication overhead.

A dynamic window scheme was presented where sensor nodes determine whether first to verify a message or to forward the message by them [8]. This is made possible with the information such as how far this node is away from the malicious attacker and how many hops the incoming message has passed in the communication network.

The basic idea of ShortPK, an efficient Short-term Public Key broadcast authentication scheme was to use short-length public/private keys but limit their lifetime to only a short period of time [9]. To cover a long period of time, more public/private key pairs are required; distributing these public keys to sensors is a challenging problem. A progressive key distribution scheme was described that is secure, efficient and packet-loss resilient. This scheme achieves a significant improvement on energy consumption.

Broadcast authentication is a critical security service in WSNs as it allows the mobile users to broadcast messages to multiple sensor nodes in the communication network in a secure way. Symmetric key based solutions such as muTESLA and multilevel muTESLA have already been proposed, they all suffer from severe energy depletion attacks resulted from the nature of delayed message authentication. Several efficient public key based schemes are presented to achieve immediate broadcast authentication and thus avoids the security vulnerability intrinsic to muTESLA. These schemes are built upon the unique integration of several cryptographic techniques including the Merkle hash tree, the Bloom filter and the partial message recovery signature scheme.

A simple, secure, dynamic, scalable, efficient and lightweight protocol (SDSEL) for mutual authentication of nodes in WSN was proposed which was based on tokens, each sensor node acquires a token from base station and later on without any involvement of base station, the sensor nodes mutually authenticate each other using acquired tokens. This protocol was modeled in scyther for verification and no potential attacks were detected.

3. EFFICIENT SECURE MANAGEMENT TECHNIQUE (ESMT)

The main objective is to send data efficiently across the network using routing strategy along with efficient security management in the Efficient Secure Management Technique (ESMT).

3.1. To improve routing efficiency

Traditional methods have performed routing by three phases: Route discovery and route maintenance. The first stable AODV protocol has only used Route Request (RREQ) and Route Reply (RREP) messages to

discover routes for data sending. Whenever a route failure occurs the route has to be entirely rebuilt causing a delay disadvantage in the system. The route discovery phase of this protocol also uses Route Request (RREQ) flooding towards the destination and the route reply message for destination.

In the proposed Efficient Secure Management Technique (ESMT) the next hop determines the Received Signal Strength RSS ($0 < RSS(n) < 100$) for a RREQ message sent by the source node and then floods the message. Similarly, the RREP message from the destination sends the node's important routing metrics, receive-rate, loss-rate and delay-rates estimated as a single Efficiency Metric (EfM) for the receiving nodes towards the direction of the source measure by equation (1).

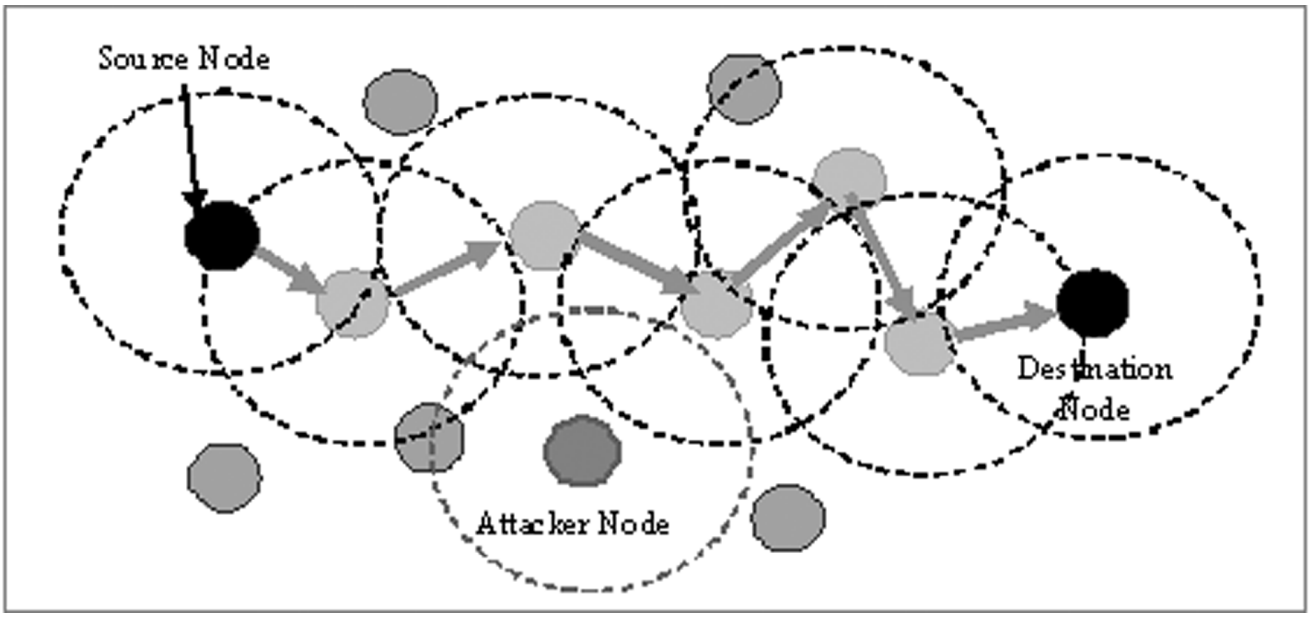

Figure 2: Scenario to illustrate the proposed ESMT

RR(n) → receive-rate of the node *n*

LR(n) → loss-rate of the node *n*

DR(n) → delay-rate of the node *n*

Therefore from these metrics the Efficiency Metric,

$$EfM(n) = RR(n) + \frac{1}{LR(n)} + \frac{1}{DR(n)} \tag{1}$$

The routes with the highest EfM(n) and distance > D_{TH} are added as a route and sent to the source where the data needs to be sent to the destination. This is intended to improve the performance of the network.

3.2. To Improve Security Management

A special random key is derived using the metrics measured for the EfM. The secret key is given by the equation (2). We substitute the value of the EfM(n) from equation (1) in the Secret key obtained in the equation (2) to get (3).

$$SKey(n) = Rand() \times Dist(n, n+1) \times EfM(n) \tag{2}$$

$$SKey(n) = Rand() \times Dist(n, n+1) \left(RR(n) + \frac{1}{LR(n)} + \frac{1}{DR(n)} \right) \tag{3}$$

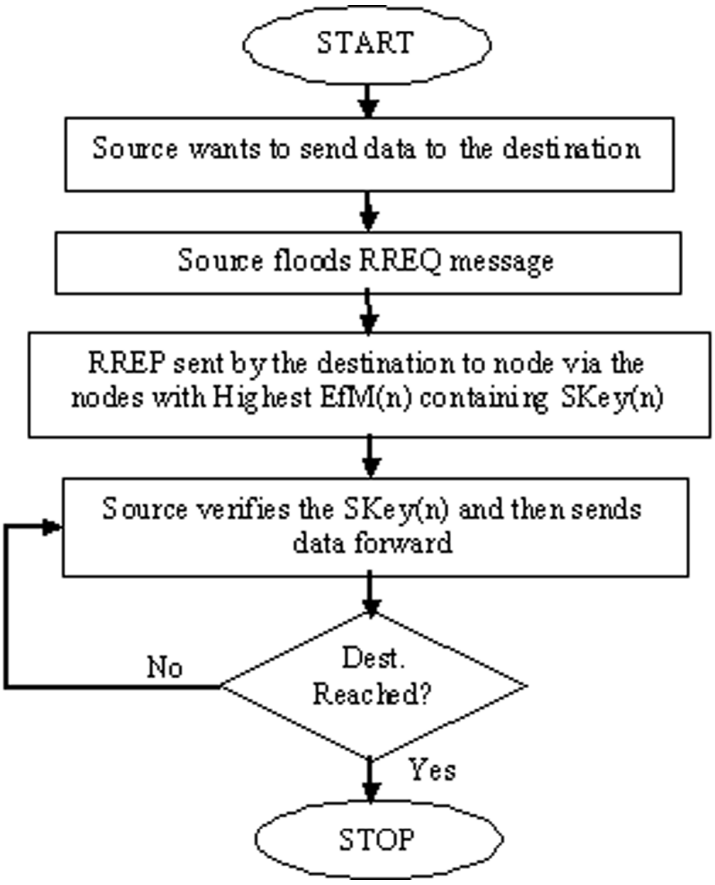

Figure 3: Working Strategy of ESMT

Where Dist(n, n + 1) is the distance between the current node n and the next node (n + 1). This is used to authenticate the communication between the nodes for communication. The nodes send data only if this particular key is verified by the nodes. The strategy by which the nodes send the data from one end to another is given in the figure 3 below.

4. SIMULATION ANALYSIS

The performance of the proposed scheme is analyzed by using the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language).

Table 1
Simulation parameters of ESMT

Parameter	*Value*
Channel Type	Wireless Channel
Simulation Time	25 s
Number of nodes	60
MAC type	802.11
Traffic model	CBR
Antenna Model	Omni Antenna
Simulation Area	1000 × 600
Transmission range	250m, 180m
Network Interface Type	Wireless PHY

NS2 is a discrete event time driven simulator which is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The nodes have to be configured as mobile nodes by using the node-config command in NS2. The parameters used for the simulation of the proposed scheme are tabulated in table 1.

The simulation of the proposed scheme has 60 nodes deployed in the simulation area 1000 × 1000. The nodes are moved randomly within the simulation area by using the mobility model Random waypoint as shown in Table 1. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay and throughput.

4.1. Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The PDR is calculated by the equation (3). The figure 4 shows that the number of packets delivered by the ESMT is greater than that of the SDEL.

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \tag{3}$$

4.2. Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The PLR is calculated by Equation (4).

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \tag{4}$$

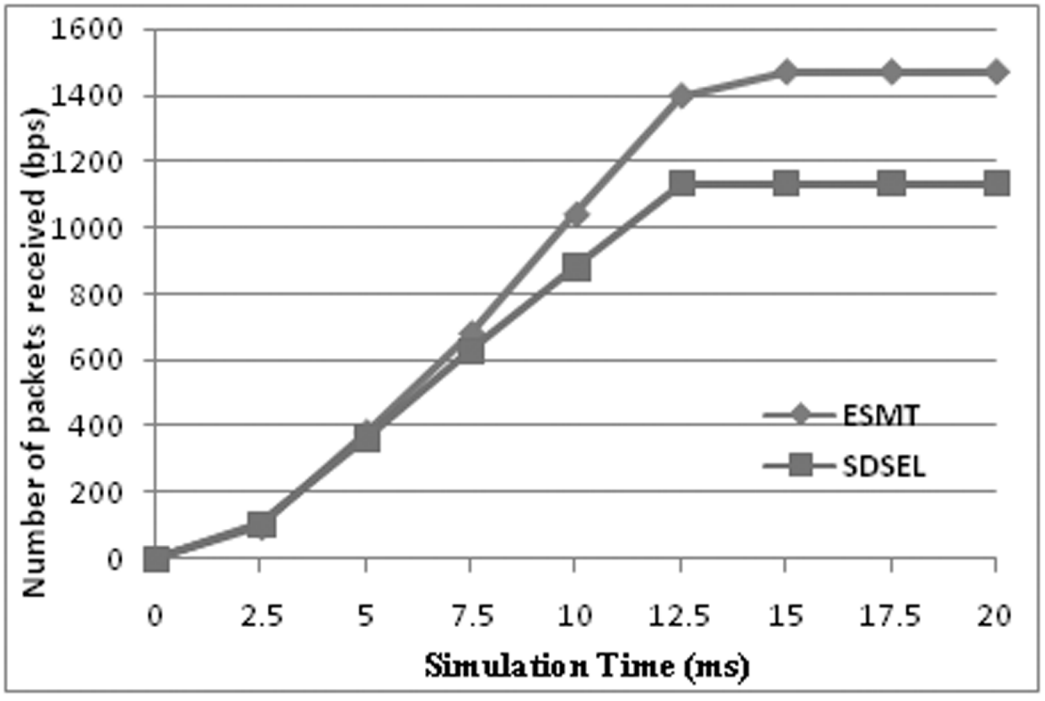

Figure 4: Packet Delivery Rate of ESMT and SDEL

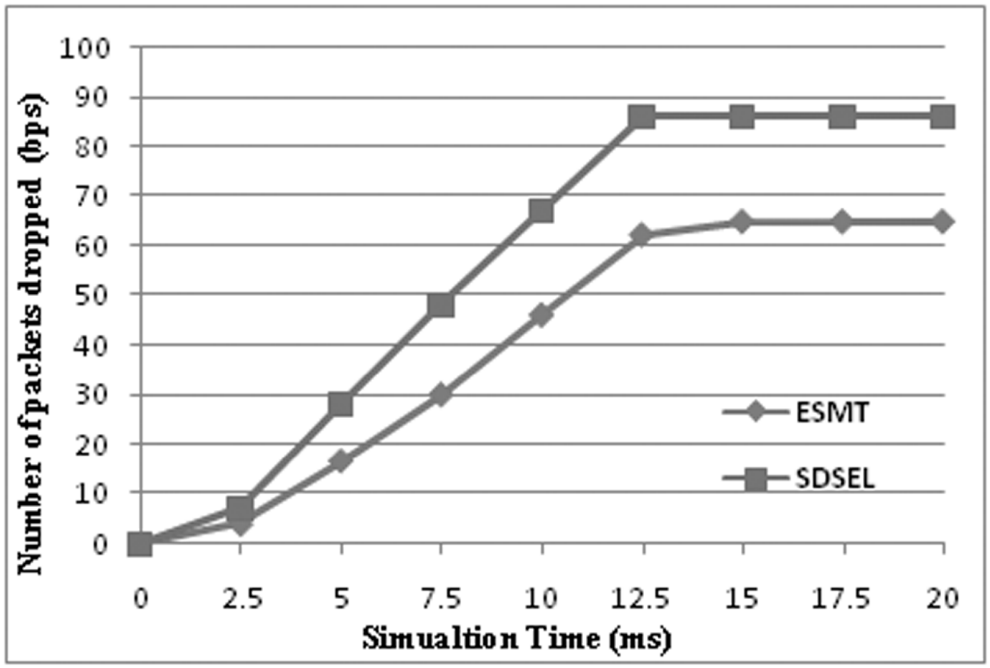

Figure 5: Packet Loss Rate of ESMT and SDEL

The figure 5 shows the packet loss rate of the ESMT protocol is lesser than that of the SDEL protocol showing the efficiency of the ESMT.

4.3. Average Delay

The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by Equation (5).

$$Average\ Delay = \frac{Pkt\ Recvd\ Time - Pkt\ Sent\ Time}{time} \tag{5}$$

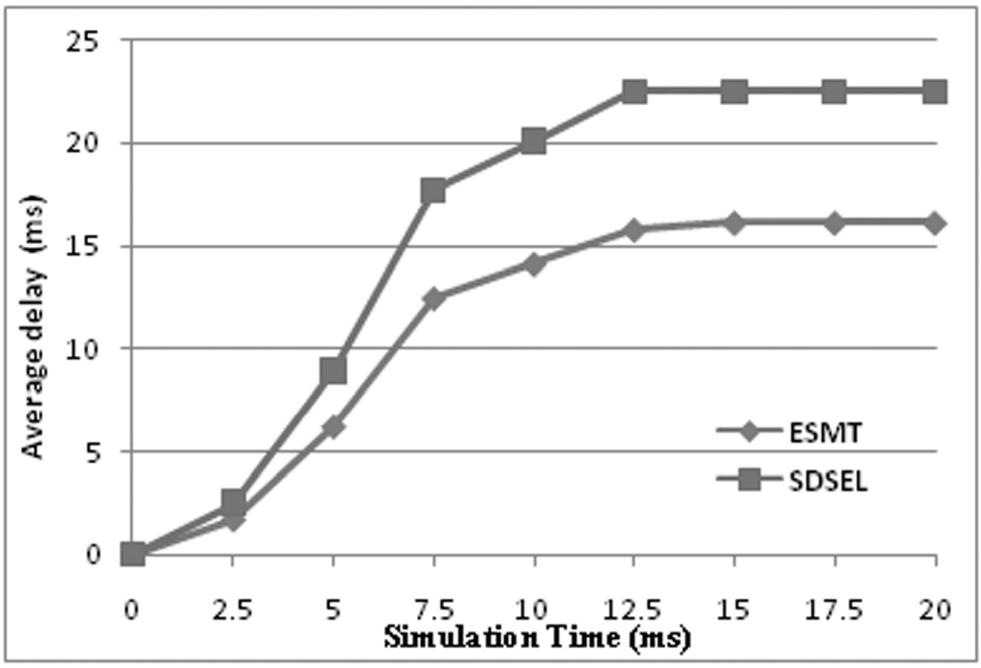

Figure 6: Average delay of ESMT and SDEL

The average delay of the SDEL is greater than the ESMT indicating the improved performance of the EMST protocol. This difference is obtained due to the incorporation of the routing efficiency and the secure mechanism in the proposed protocol.

4.4. Throughput

Throughput is the average of successful messages delivered to the destination. The average throughput is calculated using Equation (6).

$$Throughput = \frac{\sum_0^n Pkts\ Received\,(n) * Pkt\ Size}{1000} \tag{6}$$

The figure 7 shows the performance of throughput of ESMT and SDEL protocols. The throughput of the SDEL is lesser than the ESMT therefore the showing the efficiency of the ESMT protocol.

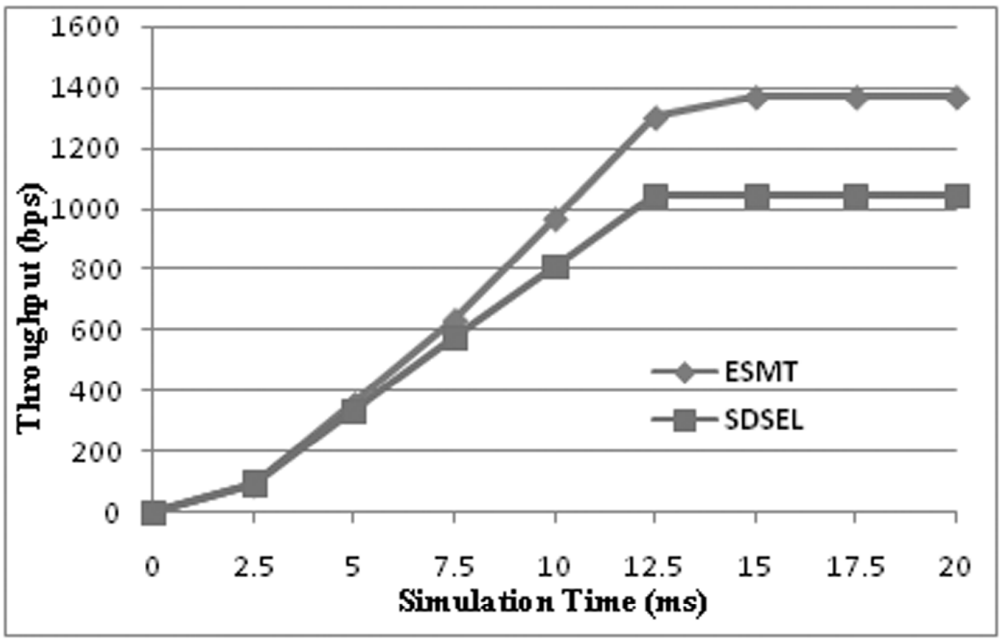

Figure 7: Throughputs of ESMT and SDEL

5. CONCLUSION

Wireless Mobile Wireless Sensor Networks (MWSNs) are one of the most recent developments in the wireless communications. There is not much work performed in the field of the MWSNs in Routing and security. Therefore, we design a new and Efficient Secure Management Technique (ESMT) for the MWSNs for node to node communication to suit different critical applications. The efficiency of this proposed method is proven in this paper using the simulations in the network simulator (NS-2). Future works can be the incorporation of Power Management techniques in the MWSNs to become a complete protocol for useful future applications.

REFERENCES

[1] K.H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,vol. 1, p. 8, Taichung, Taiwan, June 2006.

[2] X. Fan and G. Gong, "Lpkm: a lightweight polynomial-based key management protocol for distributed wireless sensor networks," in Ad Hoc Networks,vol. 111of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,pp.180–195, Springer, Berlin, Germany, 2013.

[3] O. Delgado-Mohatar, A. Fuster-Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," Ad Hoc Networks, vol.9, no.5, pp.727–735, 2011.

[4] F. Ullah, T. Mehmood, M. Habib, and M. Ibrahim, "SPINS: security protocols for sensor networks," in Proceedings of International Conference on Machine Learning and Computing (ICMLC '09), vol. 3, 2009.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks, vol. 2, no. 4, pp. 500–528, 2006.

[6] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in Proceedings of the 1st Annual IEEE Conference on Communications Society Sensor and AdHoc Communications and Networks (SECON '04), Santa Clara, Calif, USA, 2004.

[7] Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," Sensors, vol. 10, no. 4, pp. 3718–3731, 2010.

[8] R. Wang, W. Du, and P. Ning, "Containing denial-of-service attacks in broadcast authentication in sensor networks," in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing,pp.71–79,ACM, September 2007.

[9] R. Wang, W. Du, X. Liu and P. Ning, "Short PK: a short-term public key scheme for broadcast authentication in sensor networks," ACM Transactions on Sensor Networks, vol. 6, no. 1, article 9, 2009.

[10] K. Ren, S. Yu, W. Lou and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," IEEE Transactions on Vehicular Technology, vol. 58, no. 8, pp. 4554–4564, 2009.

[11] R. Rathore and M. Hussain, "Simple, secure, efficient, light-weight and token based protocol for mutual authentication in wireless sensor networks," in Emerging Research in Computing, Information, Communication and Applications,462, pp. 451, Springer, New Delhi, India, 2015.