International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

ENHANCED DYNAMIC ROUTING WITH SECURE TRANSMISSION IN WSN USING ELGAMAL SIGNATURE BASED MESSAGE AUTHENTICATION

DADALA SUMA [#1] and SHEIK AHMAD SHAH [*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science, JNTUK,A.P, India.*

[*] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— Secure data transmission is an important challenge in the wireless sensor networks. WSN comprised of huge number of sensor nodes. Each sensor node is capable of sensing its location by accumulating the information from its predecessor or successor nodes. To achieve an effective data transmission, a message authentication schemes are designed. In this paper, we make a study about enhancing the message authentication schemes based on symmetric key encryption system or public key cryptosystem. We propose "Secure Anonymous Message Authentication (SAMA)", that develops from the of ElGamal Signature key cryptosystem. It permits to transfer the data among the group of nodes without any limitation at threshold level. An experimental result assures effective message source privacy.**

***Index Terms*— Secure data transmission, Wireless Sensor Nodes, Message Authentication schemes, Symmetric key cryptosystem and Elgamal signature.**

I. INTRODUCTION

Message authentication plays a significant role in maintaining the privacy of the data transmissions in the wireless sensor networks. In the wireless sensor networks [1], communication plays a vital role. In order to perform hop by hop communication, an effective message authentication scheme is needed to prevent from unauthorized users access. [2] Though there are several message authentication schemes are available, the prevention of unauthorized user access is not yet recovered. The existing authentication schemes are limited to the high overhead, lack of ability to attack nodes and threshold problems. Message authentication plays significant task in energy consumption. By the use of symmetric key management systems [3], the message authenticity is ensured. A shared key is hold by every sender during data transmission. An attacker can easily access the key by occupying a single sensor node. So, it will does not work in multicast networks.

The sensor nodes contain huge number of nodes, so, there arise a scalability issue. In order to solve this issue [4], a secret based message authentication scheme. A delayed packet consumes a high data transfer capacity. High-reliability packages demoralize the shortest path that connects the sink while transferring and the packets with devotion requirements to reroute to maintain a strategic distance from conceivable dropping on the hotspots. Along these lines, the information respectability and postponement separated administrations can be given in the same network. Roused by this understanding, we propose the SAMA, a potential-based multi-way dynamic routing system

The rest of the paper is organized as follows: Section II describes the review of the work studied by other researchers. Section III describes about the proposed work. Section IV justifies the experimental results. At last, concluded in section V.

II. RELATED WORK

In this section, we explain about the works done in concept of symmetric key and hash based authentication schemes in the WSNs. In the single key management system, the intruders can easily access the data. The review work is explored as follows:

A. Digital signature based approaches:

The most traditional approach is the digital signature authentication and verification schemes [3]. Some public key cryptosystem are used to handle the cryptographic systems. As this system, it poses issues like high computational cost, hardware supports etc. In some scenario, arithmetic operations are used, so as to reduce the overheads [7]. The signature is invented by David Pointcheval and Jacques Stern. Using the random oracle model, they aimed to provide security schemes. They designed an algorithm for the message attacks. It combined with the ElGamal signature system that acts as security proof. It was further extended in Elliptical curve cryptography system using digital signatures. The system eliminates the threshold issue.

B. Multiple Message Authentications Code (MAC) based approaches:

The messages are authenticated by involving some hash functions into it. When compared to other security schemes, it aimed to provide better performance in terms of reduced overhead. Here, a group of nodes shares the same secret key. The nodes become useless [6-8] when it's being compromised by other nodes. However, it fails to achieve non-repudiation. Statistical en-route filtering is used for generating the false reports. Though, there is huge collection of sensor nodes are available but it unable to provide tamper resistant networks.

RAP misuses the thought of rate and proposes a velocity based scheme to minimize the proportion of missed due dates [7]. Regardless, the overall information of system topology is required. Certain Earliest Deadline To begin with (EDF) [9] [10] generally utilizes a medium access control convention to give the continuous consistent organization administration a two-jump neighbor information based edge coordinating segment is proposed to enhance ongoing execution [11]. The coordinating decision is made in perspective of the amount of ricochets from a source to the sink and the two bounce information [12].

III. PROPOSED WORK

In this section, we describe about the design of Secured Anonymous Message Authentication (SAMA) with an enhanced ElGamal Signature. The aim of this work is to authenticate the intermediate nodes so as to recover the corrupted message at the minimized level of energy consumption. In order to achieve best resilient nodes with flexible time authentication system, the novel scheme, SAMA is designed. The unique feature is that unlimited messages are authenticated without any predefined thresholds. In general, the WSNs consist of huge number of nodes.

Let us assume that each sensor nodes are aware of their original location. By the use of geographic routing, the information about the neighboring nodes is collected by intended nodes. The communications is of multi-hop system. Multihop communication that can reliably collect a large amount of data generated by the entire monitoring system to a single base-station can be made efficient with the consideration of the specific communication characteristics of physical infrastructure monitoring as well as radio interference and channel contention. Let us also consider two types of attacks namely, Passive attacks and Active attacks. Passive attacks are the attacks created by the eavesdroppers to modify the messages and analysis the network traffic. Active attacks are the attacks that are posted by the compromised nodes. In this the attackers can modify the content of the data.

The main design goals of the proposed scheme are listed as follows:

a) Authentication of the message: The transferred message is verified by both sender and receiver in mutual communication process.
b) Integrity of the message: The receiver should verify whether that the message is modified or not.
c) Message Authentication in hop-hop communication: Each forwarding node should capable of verifying authenticity and integrity of the messages.
d) Privacy Maintenance: The intruders should find difficult of compromising the nodes, to obtain sender's ID etc.
e) Efficiency: The proposed scheme should be efficient in terms of both computational and communication overhead.

The proposed SAMA algorithm based on modified ElGamal signature is given as follows:

a) The receiver node contains the encoded message.
b) The significant bits presented in the left part are in decimal format.
c) If the receiver obtains the same key, then the data are transferred via public channel.

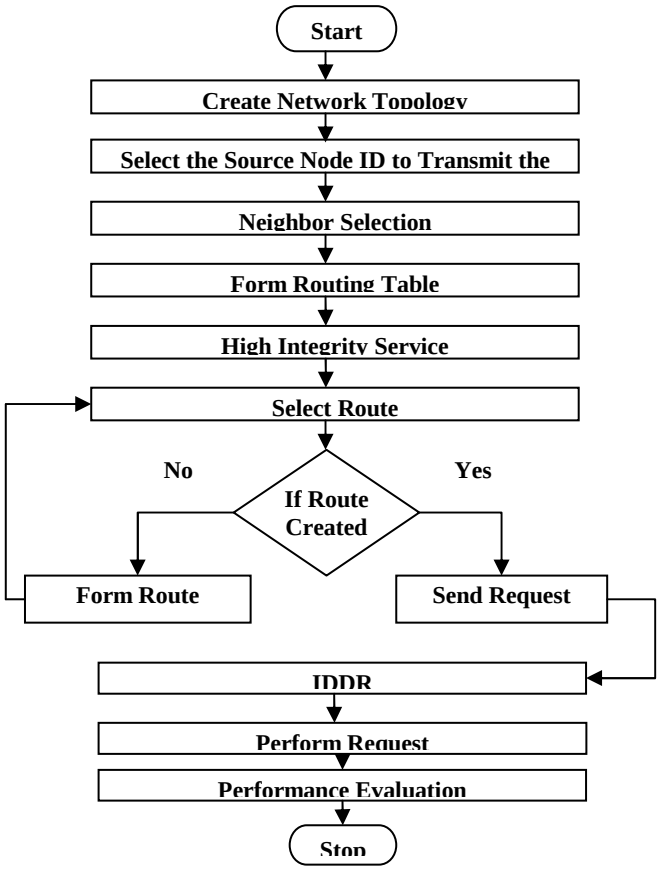

Fig. 1. Proposed System architecture

IV. EXPERIMENTAL RESULTS

The enhanced SAMA scheme using Elgamal signature is executed through simulation in NS2.The simulation parameters used for validating the proposed scheme is presented in Table1.The parameters are executed at different data rate and average data redundancy of 20% and 40%. Let us consider that similar data type of the data packets are transmitted to the Cluster Head via Base Station. The time generation for packet transmission is increased from 1 to 100pps, as the packet moves.

TABLE 1: SIMULATION PARAMETERS

Parameters	Value
No.of sensor nodes	100
Packet length	30 bytes
Buffer length	65 packets
Initial node energy	1.0J
Bandwidth	200Kb/s
Radio range	10m
Propagation	Two ray

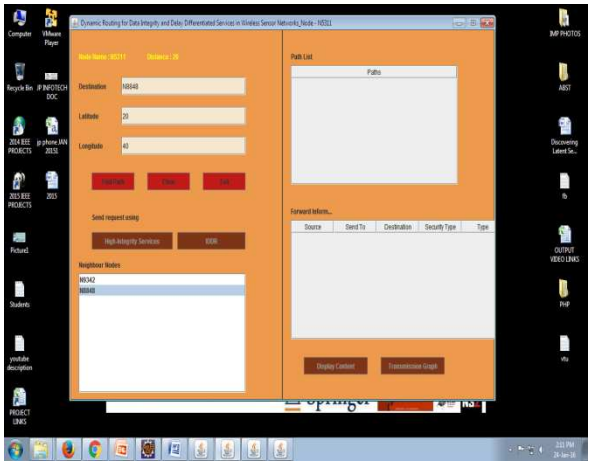

Fig.2. Collecting the information about neighboring nodes by entering the distance.

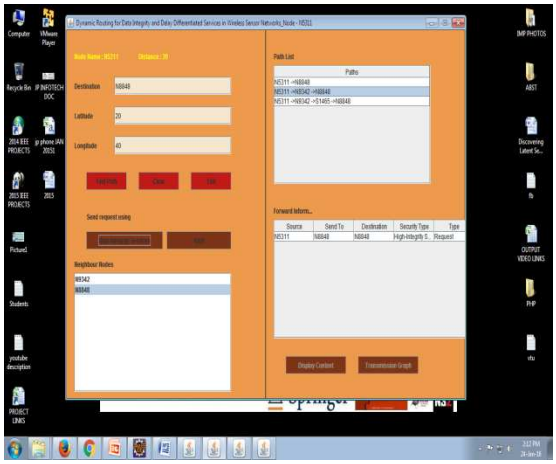

Fig.3. Working of high integrity services for secure data transmission

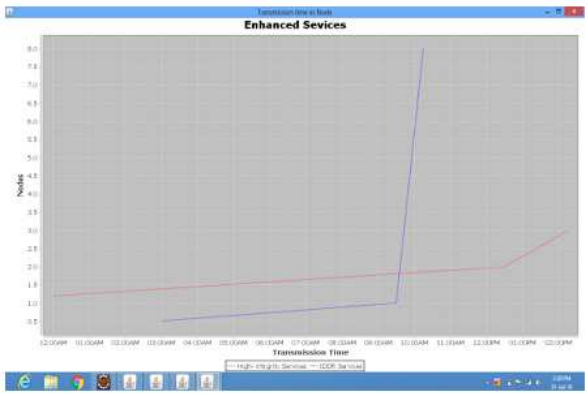

Fig.4. In proposed system the data integrity is high and delay is low.

V. CONCLUSION

In wireless sensor networks (WSN), the dynamic multipath routing is analyzed. We aim to satisfy the two different QoS requirements, high data fidelity and low end-to end delay. The result shown for transmission graph proved that SAMA can significantly enhanced the throughput of the high-integrity applications and decrease the end-to-end delay of delay sensitive applications through scattering different packets from different applications spatially and temporally. The proposed schemes also provide better scalability issue by collecting accurate local information that reduced the implementation cost. It also brings down the communication overhead. In addition, SAMA has acceptable communication overhead. It may be needed to extend the present system into a both distributed and other different types of networks by including different parameters like routing techniques, any intermediate acknowledgement service to verify the services like both delay and integrity in an efficient and effective manner.

REFERENCES

[1] P. Levis, N. Lee, M. Welsh, and D. Culler, “TOSSIM: Accurate and scalable simulation of entire TinyOS applications,” in Proc. 1st Int. Conf. Embedded Networked Sensor Syst., 2003, pp. 126–137.

[2] T. Chen, J. Tsai, and M. Gerla, “QoS routing performance in multihop multimedia wireless networks,” in Proc. IEEE Int. Conf. Universal Personal Commun., 1997, pp. 557–561.

[3] R. Sivakumar, P. Sinha, and V. Bharghavan, “CEDAR: Core extraction distributed ad hoc routing algorithm,” IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1454–1465, Aug. 1999.

[4] S. Chen and K. Nahrstedt, “Distributed quality-of-service routing inad hoc networks,” IEEE J. Selected Areas Commun., vol. 17, no. 8,pp. 1488–1505, Aug. 1999.

[5] B. Hughes and V. Cahill, “Achieving real-time guarantees in mobile ad hoc wireless networks,” in Proc. IEEE Real-TimeSyst.Symp., 2003.

[6] D. Djenouri and I. Balasingham, “Traffic differentiation-based modular qos localized routing for wireless sensor networks,” IEEE Trans. Mobile Comput., vol. 10, no. 6, pp. 797–809, Jun. 2010.

[7] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, “RAP: A real-time communication architecture for large-scale wireless sensor networks,” in Proc. IEEE 8th Real-Time Embedded Technol. Appl. Symp., 2002, pp. 55–66.

[8] M. Caccamo, L. Zhang, L. Sha, and G. Buttazzo, “An implicit prioritized access protocol for wireless sensor networks,” in Proc. IEEE Real-Time Syst. Symp., 2002, pp. 39–48.

[9] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, “SPEED: A stateless protocol for real-time communication in sensor networks,” in Proc. IEEE 23rd Int. Conf. Distrib. Comput. Syst., 2003, pp. 46–55.

[10] P. T. A. Quang and D.-S. Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks,” IEEE Trans. Ind. Inform., vol. 8, no. 1, pp. 61–68, Feb. 2012.

[11] S. Bhatnagar, B. Deb, and B. Nath, "Service differentiation in sensor networks," in Proc. Int. Symp. Wireless Pers. Multimedia Commun., 2001.
[12] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst., 2003, pp. 266–279.
[13] M. Radi, B. Dezfouli, K. A. Bakar, S. A. Razak, and M. A. Nematbakhsh, "Interference-aware multipath routing protocol for QoS improvement in event-driven wireless sensor networks," Tsinghua Sci. Technol., vol. 16, no. 5, pp. 475–490, 2011.

AUTHOR PROFILE

DADALA SUMA ,is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science). Her Area of interest includes Mobile Computing and its objectives in all current trends and techniques in Computer Science.

SHEIK AHMAD SHAH M.TECH (UCE,JNTUK) is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA. His interested areas NETWOKING, SECURITY