DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5918

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ENHANCED SECURITY FOR HOP BY HOP WIRELESS SENSOR NETWORK USING ELGAMAL ENCRYPTION ALGORITHM

J. Soundararajan
M.Sc Project Student
Department of Information Technology
Bharathiar University
Coimbatore-46, India

Dr. R. Vadivel*
Assistant Professor
Department of Information Technology
Bharathiar University
Coimbatore- 46, India

***Abstract*:** The more modern network is unidirectional, also control of sensor activity, enabling. The WSN is built or even thousands of sensors of nodes, where each node is connected to on sensors. The sensor of the WSNs, from a simple star network to an advanced multi hop wireless mesh network can vary. The collecting of the data and controlling the node, may need to perform some successive on the measured data. Direct communication between individual nodes can also be required. The Task Manager Node (User) performs tasks in data storage, analysis and display. This proposed work empowers the intermediate nodes confirm the message with the goal that all corrupted message can be distinguished and dropped to save the sensor control. Hop by hop message security method for WSN without the edge constraint of the proficient. ElGamal encryption algorithm utilized in this work enables the semantic security. This framework successfully handles all sort of security issues. It likewise gives versatility, adaptable time authentication and source identity protection without any limitation on threshold.

Keywords: WSN, SAMA protocol, ELGAMAL, Security. Elliptic curves cryptographic

I. INTRODUCTION

The performed sensor node message authentication task and submit sensing data in one time-slot to the nearest storage node while storage nodes answer and process the query from the network owner.[1] Therefore, it is important to protect the privacy and verify the query results. we define and solve the practical and challenging problem of privacy preserving and verifiable top-k query processing performed on the time-slot sensing data set in two-tier sensor network, and establish a set of privacy and correctness requirements for such a secure top-k query scheme to become a reality.[3]We propose the basic Prick Topk scheme by using order-preserving encryption, and then improve it step by step to achieve privacy.

Master nodes collect data from sensor nodes and then answer the queries from the network owner on their behalf. In hostile environments, [4] master and sensor nodes may be compromised by the adversary and return incorrect data in response to data queries. [5] Such application-level attacks are more harmful and difficult to detect than blind denial-of-service attacks on network communications, particularly when the query results are the basis for critical decision making.

II. RELATED WORK

The message authentication should be Analytical studies, numerical simulations, and prototype implementations are elative curve cryptography methods of our proposed methods. [6] The authority can issue queries to retrieve the sensor readings. [7]The middle tier is composed of a small number of storage-abundant nodes, called storage nodes. The bottom tier consists of a large number of resource-constrained ordinary sensors that sense the environment. The multipath protocol is recently mechanism for transparently supporting multiple connections to the application layer. [8] The attribute problems are linked in the traffic path. Scheme of sensitive merging in efficient manner strengths the deal between deal optimal resource pooling and impartiality [9]. It viably utilize the transmission capacity between TCP streams throughput and fairness in numerous situations, where it understands the floppiness problem [10].

The MP-TCP algorithms for mobile devices are used for the energy consumption in the real time applications [11]. The fixed duration are transferring the fixed data size. The two-timescale algorithm with theoretical will guarantee on the performance [12]. The path selection and congestion control are decides a subset path. The path selection steps are adopting the network congestion in energy consumption.

III. METHODOLOGY

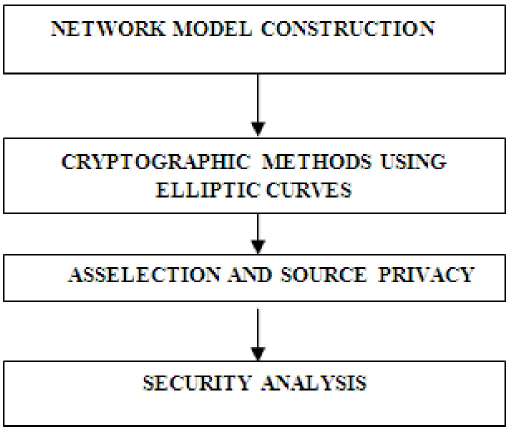
NETWORK MODEL CONSTRUCTION
CRYPTOGRAPHIC METHODS USING ELLIPTIC CURVES
ASSELECTION AND SOURCE PRIVACY
SECURITY ANALYSIS

Fig 1. Module Diagram

A. Construction of Network Model

WSNs are accepted to comprise a substantial number of sensor nodes. We expect that every sensor node knows its relative area in the sensor space and is equipped for communicating with its neighboring node specifically to utilize geographic routing. Entire network communication is completely associated with multi-hop. Also we assume that there exist a security server (SS) which is in-charge for security parameters among the system like storage, generation and distribution.

B. Elliptic Curve based Cryptographic Methods

This section describes two cryptographic strategies based on complication of discrete log issue for elliptic curves. Numerous different strategies are utilized; however we don't have options to give solutions to every issue. The strategies are for the most part additional message accessible over authentication techniques, however it give greater security per bit of information if elliptic curves are utilized.

1) Curve Selection

- Each cryptographic technique relied upon the hazard of the EC discrete log issue, it is necessary to start by selecting an elliptic curve that isn't vulnerable to the known assaults on the discrete log issue. The curve should fulfil the accompanying limitations:
- To avoid Pollard attack it's necessary to choose a prime number #E(Fq) which already exists in the security mechanism calculations. This prevents the problem from being detected from SemaevSmartSatohAraki attack.
- There exist several methods of choosing these curves.

The simplest one is to pick a curve E(Fq) : $y^2 = x^3 + ax+ b$ at random by selecting a,b $\in$ Fq such that $4a^3 + 27b^2 =0$ if q is odd and b = 0 if q is a power of 2. We then check the conditions given above. A large fraction of the time, the conditions will be satisfied. If they are not, we try a different a, b.[Bha]

C. Selection and Source Privacy

The suitable choice of an Ambiguity Set (AS) assumes a key part in message source security, since the real message source node will be covered up in the AS. Prior to a message is transmitted, the message source node chooses an AS from the public key list in Security Server (SS) as its decision. To give a protection to the message source, it needs to choose the AS which incorporate nodes from all bearings of the source node. It likewise incorporates nodes from the other way of the successor node. In this way, even the prompt successor node won't have the capacity to recognize the message source node from the forwarder in view of the message that it gets.

D. Security Analysis

Utilizing ElGamal Encryption method signature is created and the key esteem is utilized to encrypt the message and its content. However the sensor node gathers the information and location through sink node, its necessary to shroud the subtle elements of source nodes. There exists a chance for the intruder to handle the data of the source node and utilize this to trade off the security. Here, the personality of the source node is likewise hidden from the various nodes, so there is no chance to get for an intruder to estimate the attack.

$$x_k = \sum_{i=0}^{n-1} c_{i,k}\alpha^i \text{ converting into } c(x_k) = r = \sum_{i=0}^{n-1} c_{i,k} p^i, \quad 0 \le i < p.$$

Sink node continues following the message from compromised node to affirm it is compromised node. So, from the AS set it can be segregated. At the point when a node is distinguished as compromised, the SS can expel its public key from its list. Once when the public key of a node is expelled from people in public key list, any message with the AS containing the compromised hub will be dropped with no procedure to spare the valuable sensor control. Subsequently the security include gave by this approach is more practical and it upgrades the current security.

IV. SIMULATION ENVIRONMENT

The proposed method is been designed and developed using Java EE language where Java Netbeans is used as a simulator. The Java SE Development Kit (JDK) 8 is required to install NetBeans IDE. NetBeans is an open-source Integrated Development Environment (IDE)

a. Procedure

1. cryptography methods are used to the select **File** > **New**, and select the type of enterprise application you want to create:
   - Enterprise Application Project
   - Web Project
   - EJB Project
   - Connector Project
   - Application Client Project
2. To create Utility projects, select **File** > **New** > **Project ...** > **Java EE** > **Utility Project**.
3. select **File** >**New** > **Project ...** > **Web** > **Web Fragment Project.** Click **Next**.
4. In the **Project Name** field, type a name for your project.
5. In the **Target runtime** field, select your target runtime, or click **New** to create a new runtime.

V. PERFORMANCE EVALUATION

One of the aims in measuring the performance metric of the proposed elgamal encryption is to determine its scalability. Main challenging issue is how the security analysis performance varies related to the data transfer in the WSN system.

Table 1: Execution Time

Algorithm name	Execution time
ElGamal Encryption	20654
Elliptic Curve Cryptography	25853

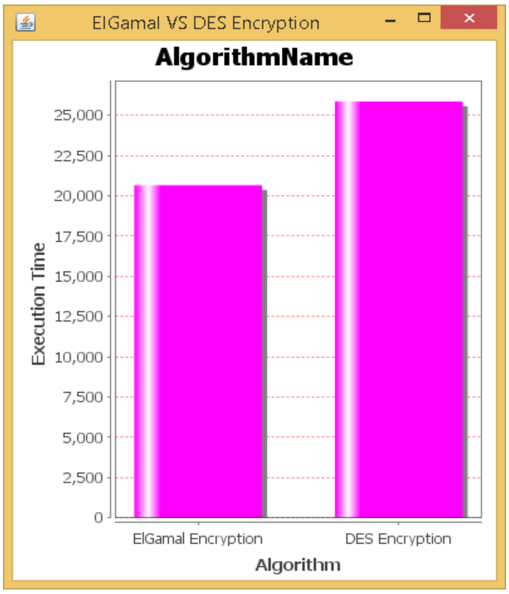

Fig 2. Elgamal and DES encryption Execution Time

Table 2: Throughput

Algorithm name	Throughput
ElGamal Encryption	8.0
Elliptic Curve Cryptography	0.1

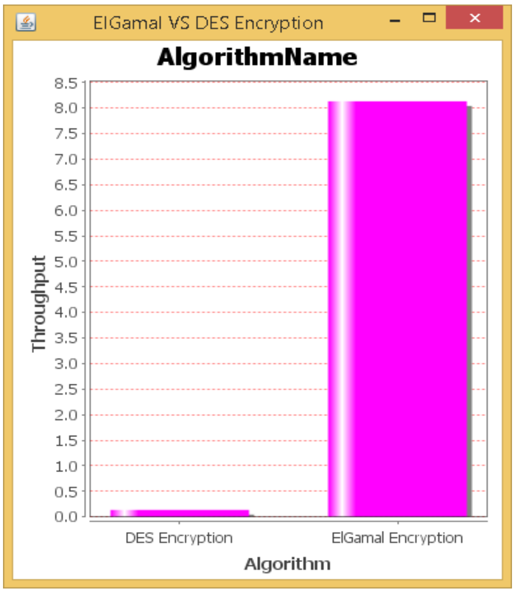

Fig 3. Elgamal and DES encryption Throughput

VI. CONCLUSION

Hop-by-Hop Message authentication was proposed in this paper to support an efficient wireless-based data transfer between multiple nodes. It consists of innovative for elgamal encryption of data from hop by hop was gracefully achieved, while secured authentication and data utilization efficiency was dramatically improved. Experimental results are tested and simulations revealed feasibility and effectiveness of elgamal encryption.

REFERENCES

[1] Chia-Mu Yu, Guo-Kai Ni, "Top-*k* Query Result Completeness Verification in Tiered Sensor Networks", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 1, January 2014.

[2] Rui Zhang, Member, IEEE, Jing Shi, Yanchao Zhang, "Secure Top-*k* Query Processing in Unattended Tiered Sensor Networks", n IEEE INFOCOM, 2010

[3] Demetrios Zeinalipour-Yazti, "Micro Hash: An Efficient Index Structure for Flash-Based Sensor Devices", USENIX Association, FAST '05: 4th USENIX Conference on File and Storage Technologies0020 (2012).

[4] Muhammad Naveed, Seny Kamara, Charles V. Wright, "Inference Attacks on Property-Preserving Encrypted Databases", ACM 978-1-4503-3832-5/15/10, 0020.

[5] J.N. Al-Karaki, Ahmed E. Kamal, "Routing techniques in wireless sensor network", IEEE Wireless Communications, Dec 2014.

[6] Muhammad Asif, , Shafiullah Khan, et al "Quality of Service of RoutingProtocols in Wireless Sensor Networks', IEEE access, Jan 2017.

[7] Ramin Khalili "MPTCP Is Not Pareto-Optimal: Performance Issues and a Possible Solution", IEEE/ACM Transactions on Networking, IEEE/ACM, 2013, pp.15, Oct2013.

[8] Qiuyu Peng**,** Minghua Chen, "Energy Efficient Multipath TCP for Mobile Devices", August 11–14, 2014, Philadelphia, PA, USA. Copyright 2014 ACM 978-1-4503-2620-9/14/08 .

[9] Eric Setton, Xiaoping Zhu and Bernd, 'Congestion-Optimized Multipath Streaming Of Video Over Ad Hoc Wireless Networks", Information Systems Laboratory, Department of Electrical Engineering Stanford University, Stanford, CA94305-9510, USA

[10] Damon Wischik, Costin Raiciu, "Design, implementation and evaluation of congestion control for multipath TCP", Conference: Proceedings of the 8th USENIX conference on Networked systems design and implementation, MARCH 2011.

[11] Anbarasan Thamizharasan Dotun Ogunkanmi, "Study the Effects of Video Frames Lost over Wireless Networks – Simulator Development", Master Thesis Computer Science Thesis no: MCS-2010-14, Jan 2010.

[12] M. Sophia Priyadarshini, A. Shobha Rekh, "Streaming Video with Multi Path TCP in Wireless Networks", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-018, Vol. 5 Issue 04, April-2016.