Accessing Multi-Model Server Based User Authentication and Key Agreement Protocol

G. Betzial Freedah
Department of Computer Science & Engineering
Bharathidasan University, Trichy, India

Abstract— Traffic patterns of wireless sensor network (WSN) usually follow many-to-one model. Sensor nodes close to static sinks will reduce their limited energy more than the other sensors, since they will have more data to send during multi-gateway transmission. This will reason network divider, isolated nodes and much shortened network lifetime. Thus, how to balance energy consumption of sensor nodes is an important research issue. Many research studies have shown that sink mobility technology can remarkable balance traffic load and improve network performance. We study the authority of network lifetime which focuses on the choice of multiple mobile sink nodes number on energy consumption and parking positions mutual authentication and key agreement scheme to overcome such a security problem, as well as their impact on performance metrics above then DoS attacks. It usually involves early stage actions such as multi-step manipulation, low-frequency susceptibility scanning, and identified compromising replica nodes. We can see that both mobile sink node numbers and the choice of parking position has important influence on network performance.

Key words: Key Agreement Protocol, Multi-Model Server based User Authentication

I. INTRODUCTION

Wireless sensor networks (WSN), are also called as wireless sensor and actuator network (WSANs), are spatially distributed independent sensors to screen physical and environmental conditions, such as temperature, sound, pressure, etc. to supportively pass their data to the main location through the network. The more modern networks are bi-directional, also enabling control of sensor activity. The evolution of wireless sensor networks was motivated by military applications today such as battlefield shadowing. Such networks are used in many industrial and consumer applications, which can include industrial process and machine health monitoring and control, so on.

A. Security

In networks, network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, change, or denial of the computer network and network-accessible resources. The authorization of access to data onto a network involves network security, which is controlled by the administrator. The Users choose or the user is assigned an User_ID and password or other authenticating information that allows them to access the information and programs within their specialist. Network security covers a variety of computer networks, both public and private, that is used in everyday jobs conducting transactions and communications among the individuals, businesses, government organizations. Private networks, such a company and others which might be open to public access. Organizations, enterprises, and other types of institutions involve in network security.

Key agreement schemes are used extensively for various kinds of multi-way communication, and to detect the authenticity of the sender of any message. Key agreement protocols are needed in various kinds of communication. Keys need to be securely exchanged before a communication establishment. Security threats namely intruder-in-the-middle, where the adversary act as if someone to both the communicating parties. Replays of old keys are another attack that is common. Thus this is the reason to develop secure key protocols for exchanging information to establish secure communication.

B. Energy Model

In WSNs, the sensor nodes are being powered by small batteries and recharging or replacing the batteries, as the sensor nodes are organized in aggressive environment for many applications. Although it is a challenging task, but for the prolonged network service, the energy conservation especially of the sensor nodes of the WSNs, are required. The main components of sensor nodes are a micro-controller, transceiver, peripheral memory, power source and one or more sensor(s), where the transmission of the themes involve transceiver.

C. Security Monitoring

Sensor network application is a security monitoring. Throughout an environment Security monitoring networks is formulated of nodes that are placed at fixed locations that continually monitor one or more sensors to detect an anomaly. A key dissimilarity between the security and environmental monitoring is that security networks are not really collecting any data. This has a significant impact on the ideal network architecture. Each node has to often check the status of its sensors but it only has to send a data report when there is a security abuse. The instant and reliable communication of alarm messages is the primary system need. These are "reported by exception" networks.

D. Node Tracking Scenarios

The track of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to path the site of valuable assets or personnel. Current inventory control systems challenge to track the objects by copying the last checkpoint that an object passed through. However, with these systems it is not possible to find the current place of an object. For example, UPS tracks every shipment by scanning it with a bar code when it passes through a routing center. The system breaks down when objects do not flow from checkpoint to checkpoint. In a work environment, it is not practical to expect objects to be continually passed through checkpoints.

Keystroke dynamics systems are used for two different purposes. Firstly: identification, which is a way of determining the user's identity when no data is available about their identity beforehand. In this method, a test sample

is matched with all the templates stored in a database. The system assigns the user to the identity of the person whose template is the most similar to the test sample. The second purpose are authentication which is used to verify the identity of the user.

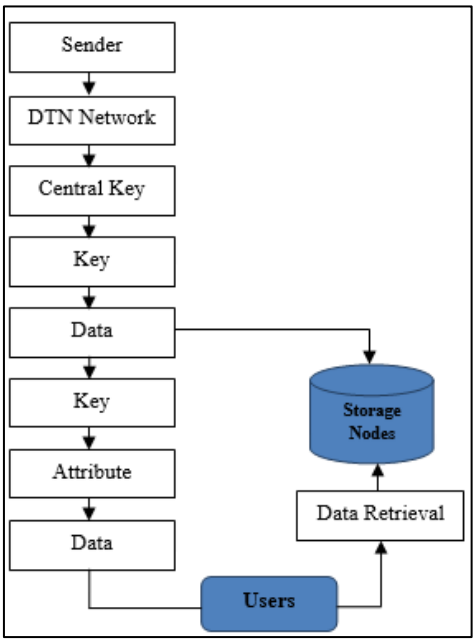

Fig. 1: Node Tracking Scenarios

II. Algorithm for Key Generation

A trusted party chooses and publishes a prime p and an integer having large prime order in F*p 1. Select a large prime number p. i. Choose a secret integer a. ii. Compute A ≡ ga(mod p). iii. Choose a secret integer b. iv. Compute B ≡ gb(mod p). 2. Masters (secret key) Compute the number Ba(mod p). Compute the number Ab(mod p). The shared secret value is Ba ≡ (gb)a ≡ gab ≡ (ga)b ≡ Ab(mod p).

A. Data Encryption

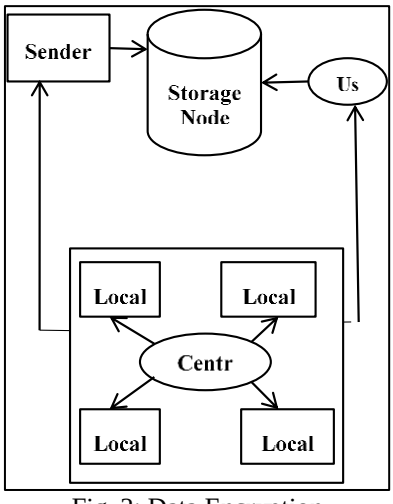

Fig. 2: Data Encryption

When a sender wants to deliver its confidential data M, he defines the tree access structure T over the universe of attributes L, encrypts the data onto to enforce attribute-based access control on the data, and stores into the storage node. The encryption algorithm takes as inputting the message M, public parameter PK and access structure A over the creation of attributes. Create the output CT such that only those users that had valid set of attributes that satisfy the access policy can only able to decrypt. Accept that the CT obliquely contains access structure A.

B. Data Decryption:

The user decrypts the cipher text with its secret key when a user receives the cipher text from the storage node. It takes input the public parameter by user using decrypt algorithm, the cipher text CT includes the access structure A and the secret key SK contain of user attribute set S. If S fulfills the access tree then algorithm decrypt the CT and give M otherwise gives "ϕ". Key Update (MK, SK, old value, new value): The key updating algorithm runs by CA. It takes as input the master key of CA, old SK and old attribute value old value, and then updates the secret key SK by updating (add/delete/update) old value with new value.

Encryption and decryption of a data should be analyzed and measured with the computational cost. Benchmark timing should be included in each activity. Each cryptographic operation was applied using the PBC library ver. 0.4.18 on a 3.0-GHz processor PC. The public key parameters were convinced to provide the 80-bit security level. The computational cost is analyzed in expressions of the pairing, exponentiation operations. The comparatively negligible hash, symmetric key, and multiplication operations in the set are ignored in the time result the computational time results. For each operation include benchmark timing.

III. Experimentation and Results

In this paper uses multiple dataset where some of them are existing dataset and some of them are new dataset. For the implementation of multi-gateway network by using Network Simulator tool.

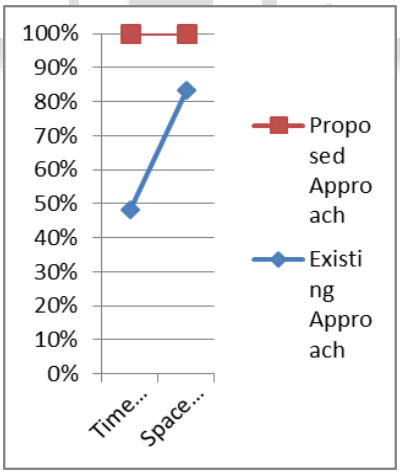

Fig. 3: Results

The performance of the proposed work is compared with the existing approach and its results are mentioned as above. From that graph the proposed work has provides better results based on time and space complexity.

IV. Conclusion

Wireless sensor networks play a major role in security. Message authentication plays a key role in thwarting unauthorized and ruined messages in the network from being forwarded to save the precious sensor energy. In the WSNs environment, the challenge is to provide an efficient security aspect that are in the research field and many researchers still

try to improve the efficiency of the system. The network is formed by a large number of tiny sensors, randomly scattered over an area where sink positioned at the center. The sensors produce data with the same rate and the data travels from the nodes to the sink in a multi-gateway network, using a shortest path routing. This protocol is mainly considered as a key exchange scheme. It is directed to be weak to man-in-the-middle attack. Then we showed how to avoid this attack by using an encryption/ decryption.

REFERENCE

[1] Junqi Zhang1,2, Rajan Shankaran1, Mehmet A. Orgun1, Abdul Sattar2, and Vijay Varadharajan1," A Dynamic Authentication Scheme for Hierarchical Wireless Sensor Networks".
[2] Nithya Menon, S.Praveena," BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013,pp.112-115.
[3] Prof N.R.Wankhade, Jadhav Ashvini B.," A Survey Paper on Hop by Hop MessageAuthentication in Wireless Sensor Network" , N.R.Wankhade et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8321-8324.
[4] Ashwini M. Rathod1, Archana C. S., "Secure Network Discovery by Message Authentication in Wireless Sensor Network", International Journal of Research in Engineering Technology and Management, pp.1-7.
[5] M. H¨olbl, and T. Welzer. Two improved two-partyidentity-based authenticated key agreement protocols. Computer Standards& Interfaces, Volume 31, 2009, Pages 1056-1060.
[6] Y. Chen, J. Chou, and C. Huang. Improvements on two password-based authentication protocols. Cryptologye Print Archive, 2010.
[7] P. Nose. Security weaknesses of authenticated key agreement protocols. Information Processing Letters Volume 111, Issue 14, 31 July 2011, Pages 687–696.
[8] B.T. Hsieh, H.M. Sun, T. Hwang, C.T. Lin. An improvement of Saeednia's identity based key exchange protocol. Information Security Conference 2002, 2002, pp. 41–43.
[9] Y.M. Tseng. An efficient two-party identity-based key exchange protocol.Informatica 18 (1) (2007) 125–136.
[10] W. Diffie, M.E. Hellman. New directions in cryptography.IEEE Transactions on Information Theory 22 (1976) 644–654.
[11] H. Shih. Cryptanalysis on Two Password Authentication Schemes.Master'sThesis.Laboratory of Cryptography and Information Security Department of Computer Science and Information Engineering.NationalCentral University, Chung-Li, Taiwan 320, Republic of China.
[12] W. Stallings. Cryptography and Network Security, 4/E. Prenti

