International Journal of Advanced Trends in Computer Applications
www.ijatca.com

KEY MANAGEMENT

Shazia Shamas [1], Ms.Yojana Chandel [2]
[1] Research Scholar
[2]Lecturer
[1,2]Computer Science Department
Panchkula Engineering College, KU
Haryana,India
[1]*shaziakashmir001@gmail.com*,[2]*yojnachandel@gmail.com*

Abstract: *Key Establishment in WSN in today's world has become more important due to advancement and need of better communication system. Due to this reason it has become important to find a means by which the communication is faster, more accurate and more secure.RSA encryption and decryption method and HLA authenticator can be used with key establishment to enhance communication system.*

In this proposed thesis work we have created a network system of 100x100 area which contains approx 100 nodes. Data is transferred from source to destination using key establishment, bit map, RSA and HLA Technique at the decryption side reverse process is applied to retrieve the transmitted data. If there is any fault in node or in link of nodes or any type of failure in network system it can be easily traced and corrected. Keys are established in such a way that it prevent the network system from attacks. For this type of key establishment cluster key establishment technique has been used. The previous work is compared on the basis of various parameters like Average localization error, root mean square error and energy efficiency or accuracy. For proposed work MATLAB software has been used.

Keywords: *WSN, Key Management, HLA, RSA, Cluster Key Management.*

I. INTRODUCTION

Wireless sensor networks (WSN) comprising of little gadgets known as micro-sensors, which collects data by collaborating with one another [7]. These little detecting gadgets are termed as nodes. Nodes essentially have three primary parts, CPU (for data handling), memory (for data stockpiling), battery (for vitality) and transceiver (for accepting and sending signs or information starting with one node then onto the next). The extent of every sensor node differs appropriately with applications. For instance, in some military or reconnaissance applications it may be little. Its expense relies on upon its parameters like memory size, processing speed and battery [5]. The normal building design of the sensor node is shown in figure 1.1.

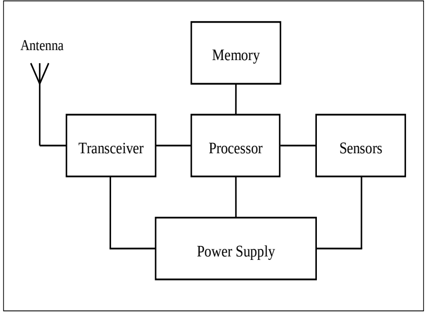


Fig 1.1: Sensor Node Architecture

The utilization of remote sensor system is expanding step by step and in the meantime it confronts the issue of vitality imperatives as far as constrained battery lifetime.

The accompanying steps can be taken to spare vitality brought on by communication in wireless sensor systems.

To plan the node's condition (i.e. transmitting, receiving, idle or sleep).

Changing the transmission reach between the detecting hubs.

Utilizing productive routing and information gathering techniques.

Avoiding the handling of undesirable information as on account of overhearing.

In WSNs, battery is the main wellspring of life for the hubs. Speaking with different hubs or sensing activities devours a great deal of vitality in processing the information and transmitting the gathered information to the sink. Much of the time (e.g. observation applications), it is undesirable to supplant the batteries that are exhausted or depleted of vitality. Numerous analysts are in this manner attempting to discover power-aware conventions for remote sensor systems with a specific end goal to overcome such vitality productivity issues as those expressed previously. Every one of the conventions that are outlined and actualized in WSNs ought to give some ongoing backing as they are connected in regions where information is detected, handled and transmitted in light of an occasion that prompts a quick activity [2]. It ought to give repetitive information to the base station. The base station or sink utilize the information that is gathered among all the detecting hubs in the system. The postponement in transmission of information from the detecting hubs to the sink ought to be little, which prompts a quick reaction.

Components of WSN::

The main components of a general WSN are the sensor nodes, the sink (Base Station) and the events being monitored. Where the communication among the nodes is low-power wireless link while the communication between the base stations low latency and higher bandwidth link.

1.2.1 Base Station (Sink) (BS)

Practically, the use of multiple base stations decreases network delay and performs better using robust data gathering [1].

1.2.2 The Sensor Nodes

As shown in the Fig. 1.2, a sensor node is composed of four basic components: sensing unit, processing unit, transceiver unit and a power unit.

WSN Application

Propels in wireless sensor networking and incorporation have empowered little, adaptable, minimal effort hubs that cooperate with their surroundings through sensors, actuators and correspondence. An applications' portion are talked about beneath in point of interest.

Habitat Monitoring: Habitat monitoring gives a wide gathering of detecting modalities and ecological conditions.

Physiological Monitoring: The advancements in embedded biomedical or physiological gadgets and brilliant coordinated sensors make the utilization of sensor systems for biomedical applications conceivable.

Vehicle Tracking: WSNs can be conveyed to track the vehicles inside of a geographic district.

Industrial Applications: The rise of WSN has had a major effect on industrial fields for example, industrial sensing and control applications, building automation, and access control.

II. LITERATURE SURVEY

Baojiang Cui et al. (2015) [6], in this study, a basic key management protocol is described for WSNs based on four kinds of keys, which can be derived from an initial master key, and an enhanced protocol is proposed based on Diffie-Hellman algorithm. The proposed scheme restricts the adverse security impact of a captured node to the rest of WSNs and meets the requirement of energy efficiency by supporting in-network processing. The master key protection, key revocation mechanism, and the authentication mechanism based on one-way hash function are, respectively, discussed. Finally, the performance of the proposed scheme is analyzed from the aspects of computational efficiency, storage requirement and communication cost, and its anti-attack capability in protecting WSNs is discussed under various attack models. In this paper, promising research directions are also discussed.

Vikash Kumar et al. (2014) [5], the intent of this paper is to investigate the security related issues, the challenges and to propose some solutions to secure the WSN against these security threats. While the set of challenges in sensor networks are diverse, this paper focus only on the challenges related to the security of Wireless Sensor Network. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed.

X. He et al. (2013) [7], authors presented an overview of state of the art dynamic key management schemes in WSNs. With the wide application of WSNs, as one of the fundamental security issues, dynamic key management is attracting more attention from the researchers and industrial engineers and many schemes were already proposed. They discussed the basic requirements of dynamic key management in WSNs, surveyed the proposed schemes for these environments and highlighted the security and performance advantages and disadvantages of each scheme. Finally, they have summarized and analyzed these techniques according to the discussed evaluation metrics. In summary, it is not possible to find one single perfect scheme can perform well in all evaluation metrics as each of them has some definite strengths, weaknesses and suitability for specific situations. The ultimate objective of this study is to encourage more researchers to design and improve potential proposals in dynamic key management for wireless sensor networks.

Krzysztof Daniluk et al. (2012) [8], in this paper, authors focus on energy aware security architectures and protocols for use in WSNs. To give the motivation behind energy efficient secure networks, first, the security requirements of wireless sensor networks are presented and the relationships between network security and network lifetime limited by often insufficient resources of network nodes are explained. Second, a short literature survey of energy aware security solutions for use in WSNs is presented. Thus, due to scarce resources, unique properties of wireless sensor networks, and often hostile environments it is a challenging task to protect sensitive information transmitted by nodes forming a WSN. Due to limited resources of nodes that form WSN many solutions providing strong security are impractical in this type of network.

Z. Ming et al. (2012) [9], To tackle the problems of excessive computation overhead and storage space and inflexible management adhering to the existing wireless sensor networks, a cluster based dynamic key management scheme is proposed based on the clustered network topology and virtual grid technology. Within the scheme, the communication between the cluster head and the active nodes is conducted using pre-distribution strategy of the head key, and the communication between cluster heads is conducted using, pair-wise key based on the combination of Blom matrix and random numbers. The scheme can dynamically update the key when the active nodes or cluster heads are captured or their energy is used up. Compared with the existing schemes, the proposed scheme can dynamically update the key and is of higher security and good scalability.

III.PROBLEM FORMULATION

Individual key is a unique key of each sensor node that shared with the controller (the base station) which is used for individual authentication and secure communication assurance. Since every node in the network shares a unique individual key with the base station, it is neither practical nor efficient to store all these keys for the base station especially when the network scalability is very huge. Thus, it is important to adopt a strategy to reduce the storage overhead, which can be achieved by the key generation function. Earlier the group key Kg is used for encrypting messages that need to be broadcasted to the whole group. This approach is different from other approaches; the key point here is no longer about key establishment or encrypting schemes because there is only one group key shared among the entire network; meanwhile it does not make sense to encrypt a broadcast message using master key of each sensor node separately.

Pairwise keys of a node indicate the keys shared with each of its direct neighbors, so the storage overhead of such keys for each node depends on the number of its neighbors.

OBJECTIVES

The security detection in WSNs is more difficult than in other systems since sensor systems are often deployed in unattended environments. Thus, the survivability of the network is one of most important security requirements when compromised nodes are not detected.

The protocols proposed should be scalable and provide efficient and enough storage space, along with efficient communication and computation.

With the approach proposed i.e. cluster key establishment technique, an outside attacker cannot succeed in launching wormhole attack except in the neighbor discovery process. Because the time of neighbor discovery process is very short (probably in seconds), the probability that the attacker achieves such attacks is also quite small. If an inside attacker compromises two or more nodes, it can launch such attacks. However, it cannot convince two distant nodes as neighbors when the neighbor discovery phase is finished. The authenticated neighborhood information is critical to deal with the wormhole attacks.

Improved Technique

RSA (Cryptosystem)

RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. In RSA, the encryption key is public and differs from the decryption key which is kept secret. A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages.

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. RSA involves a public key and a private key. The public key

can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The basic principle behind RSA is the observation that it is practical to find three very large positive integers e,d and n such that with modular exponentiation for all m:

$$(m^e)^d \pmod{n} = m$$

and that even knowing e and n or even m it can be extremely difficult to find d. Additionally, for some operations it is convenient that the operation is symmetric in that this relation also implies that:

$$(m^d)^e \pmod{n} = m$$

1.Key distribution: To enable Bob to send her encrypted messages, Alice transmits her public key (n, e) to Bob via a reliable, but not necessarily secret route, and keeps the private key d secret and this is never revealed to anyone. Once distributed the keys can be reused over and over.

2.Encryption: Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ and gcd(m, n) = 1 by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done efficiently, even for 500-bit numbers, using modular exponentiation. Bob then transmits c to Alice. Note that at least nine values of m will yield a ciphertext c equal to m.

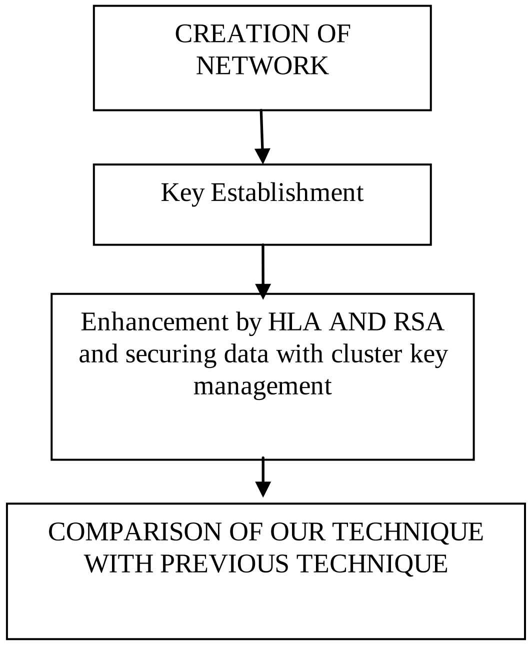
3.Decryption: Alice can recover m from c by using her private key exponent d by computing

$$c^d \pmod{n} \equiv (m^e)^d \pmod{n} \equiv m$$

Given m, she can recover the original message M by reversing the padding scheme.

The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q, are generated using the Rabin-Miller primarily test algorithm. A modulus n is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length. The public key consists of the modulus n, and a public exponent, e, which is normally set at 65537, as it's a prime number that is not too large. The e figure doesn't have to be a secretly selected prime number as the public key is shared with everyone. The private key consists of the modulus n and the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

Flow Chart


CREATION OF NETWORK
Key Establishment
Enhancement by HLA AND RSA and securing data with cluster key management
COMPARISON OF OUR TECHNIQUE WITH PREVIOUS TECHNIQUE

Step 1: Nodes are deployed and path is defined between source to destination thus network system is created.

Step 2: Keys are established in such a way that it prevent the network system from attacks. In Proposed Work Cluster Key establishment has been used.

Step 3: RSA i.e. A type of Cryptosystem is most common type which uses Encryption and Decryption Technique. Homomorphic Linear Authenticator is a type of authenticator to find malicious node.

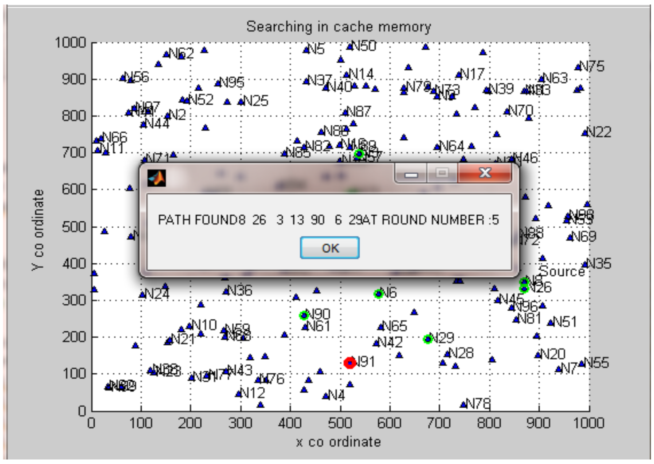
Step 4: Comparison of proposed with previous approach.

False alarm probability- It shows the false alarm raised even if all the nodes are in proper condition or all the data transferred from source to destination are not distorted by any type of error.

Overall Detection Error Probability- It shows error in detecting the fault due to which data was not being transferred from source to destination.

Malicious Packet Dropping Rate- The rate or speed by which data is lost due to malicious nodes.
Accuracy – It shows the error which occurred in transmission of data with respect to total data transferred.

IV. RESULTS



PATH FOUND8 26 3 13 90 6 29AT ROUND NUMBER :5

Fig 1.2: Creation of nodes and shortest path.

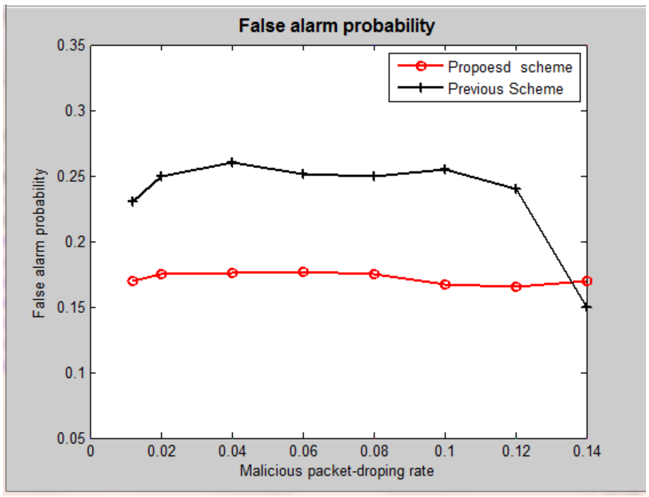


Fig 1.3: Reduction in False alarm probability

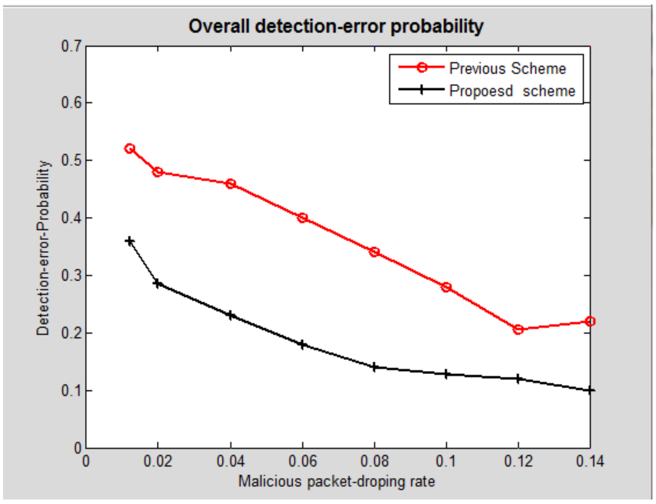


Fig 1.4: Reduction in overall detection-error probability

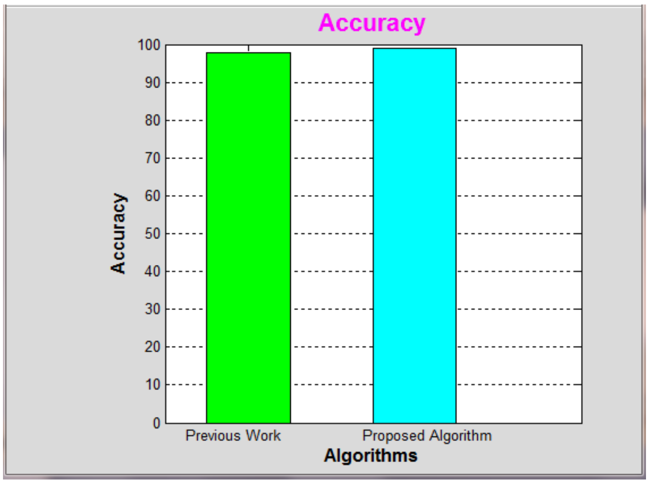


Fig 1.5: Improvement in accuracy in comparison to previous work done.

V. CONCLUSION

There are different types of approaches used with each has its advantages and disadvantages. We cannot say that one approach provides best result upon other but we will use cluster key establishment technique and achieve better accuracy result. Cluster key management technique is proposed, which assumes that the attacker cannot compromise a node in a short time. It satisfies various security requirements of WSNs using the combination of secure keys.

FUTURE SCOPE

As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas.

REFERENCES

[1] Hemanta Kumar Kalita and Avijit Kar, “Wireless Sensor Network Security Analysis”, International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[2] Yun Li, Nan Yu, Weiyi Zhang, Weiliang Zhao, Xiaohu You, Mahmoud Daneshmand, “Enhancing the performance of LEACH protocol in wireless sensor networks”, Lab. of Wireless Networks, Chongqing Univ. of Posts & Telecommun., Chongqing, China, Conference: Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference on Source: IEEE Xplore, Page no. 223 – 228, 2011.

[3] Krzysztof Daniluka and Ewa Niewiadomska-Szynkiewicz, “A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks”, Journal of Telecommunications and Information Technology, March 2012.

[4] M. Golsorkhtabar, F. K. Nia, M. Hosseinzadeh, Y. Vejdanparast, “The Novel Energy Adaptive Protocol for heterogeneous wireless sensor networks”, Computer Science

and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume: 2), Page no. 178 – 182, July 2010.

[5] Vikash Kumar, Anshu Jai and P N Barwal, “Wireless Sensor Networks: Security Issues, Challenges and Solutions”, International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8, pp. 859-868, International Research Publications House, 2014.

[6] Baojiang Cui, ZiyueWang, Bing Zhao, Xiaobing Liang, and Yuemin Ding, “Enhanced Key Management Protocols for Wireless Sensor Networks”, Hindawi Publishing Corporation Mobile Information Systems Volume, Doi: 10.1155/2015/627548, 2015.

[7] X. He, M. Niedermeier, and H. de Meer, “Dynamic key management in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol. 36, no. 2, pp. 611–622, 2013.

[8] Krzysztof Daniluka and Ewa Niewiadomska-Szynkiewicz, “A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks”, Journal of Telecommunications and Information Technology, March 2012.

[9] Z. Ming, W. Suo-ping, and X. He, “Dynamic key management scheme for wireless sensor networks based on cluster,” Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 32, no. 1, 2012.

[10] Deepika Gogia, Dr. Kamal Sharma, Deepak Kumar, “Zonal circular LEACH Protocol (ZCLP) for Homogeneous WSN”, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 1, Issue 1, June 2014, pp. 65-69

[11] A. Savvides, C-C Han, aind M. Srivastava, ”Dynamic localization in Ad-Hoc networks of sensors," Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 166-179, July 2001.