ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Securing Source Privacy in WSN by Dynamic Path Activation Based on Message Authentication

K.Malathi[1], C.M.Shamily[2]

Assistant Professor, Department of Computer Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India[1]

PG Scholar, Department of Computer Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India[2]

ABSTRACT: The message authentication is the method which promises the user that the message is transferring from the trusted user. The recent days there are a choice of methods for authentication such as Message Authentication Code, Key Aggregate System and Signcryption are appear very speedily for better security precaution. This survey paper focuses the hop by hop message verification in wireless sensor networks environment. The Wireless ad hoc networks are the end of attention of many researchers regarding the security issue in the past several years. This hop-by-hop message authentication scheme is efficient and reliable for the data transfer over the network. There were several methods have been developed to resolve the problem such as private and public key cryptography.

KEYWORDS: Hop-by-hop authentication, public-key encryption, Key Distribution Model, wireless sensor networks (WSNs).

I.INTRODUCTION

The wide variety of Wireless Sensor Networks will detect and removes the unwanted and undesirable changes that are present in the compromised node which remains as a great challenge in the research. It enables the attacker to access all the security information's that are being stored in the compromised nodes. Finally the duplicate report is successfully generated by the compromised nodes and it is compared with the neighbour nodes, which has no way to differentiate the duplicate report with the appropriate ones. Although a mechanism named public key cryptography is used, so that this mechanism will call back or rescind any key among the compromised nodes. In substantiality the summing and repository of actuator nodes hinge on asymmetric cryptography.

The Distribution of key is very complicated in cryptography and it plays a major role in the distributed system especially for security purpose in networking. The cumulating of bandwidth, size and usage in the distributed systems postures new innovative ideas in the networks. An expanding application area in networking is confronting a bundle of entities that collude individually in a bilateral procedure (such as bulletin board)

The Assorted Distribution of keys has been illuminated essentially to pairs of users. The secure and straightforward scheme will distribute keys to the users in such way the common key is shared by the group of users. In occasion of session keys the number of users will ne denoted by n, then the server produce n (n-1)/2 keys which is hold by each and individual users for communication.

In appliance to the sensor networks, the sensor nodes acts as a major challenge in some of the security mechanisms. It have finite battery life, comparably low computational power, and narrow memory in a momentous frame of research for specialized purpose is fixate, high comfortable for some of the application in the sensor networking.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

II. LITERATURE SURVEY

PSDM is the technique that has been proposed simultaneously. Therefore, to solve this problem many scholars has been introduced for several explanations that lies under a multiple division depends on the Electronic Health Record. The first part of secure Access computation issued the greater level of secure privacy that enables the entities that reveals a group of information without collecting the entity of an individual's input and the output for data mining techniques. Data mining techniques are executed by using universal techniques.

The protected multiparty calculation work for the members who are taking part to safeguard certain functions for computing the appropriated and confidential inputs. Now the question occurs is, does the computing calculation is confidential?

One way to solve this question is to preserve some of the properties related to security. Such property often occurs in sequestration or authority.one of the attempt to characterize the privacy is, the input that are generated by one party must taught the way of generating the input for another party. Therefore, this process is done just because of the information's from another parties input. Finally, there is a recruitment for privacy is formalized by telling that the information's are taught only by the parties in the computing calculation. This can be done only by output function. Therefore, privacy is the secure property that occurs very rarely. Another property is that of definiteness, which states that the output parties are mentioned by the function. Then the untrusted party are capable of receiving the tree that are altered to provide the leading information. We stress that moving with these types of properties is very hard, and it takes several years till we are persuaded.

A. *THREAT MODEL*

In threat model, invader know the security mechanisms that are arranged in Wi-Fi Networks, that is capable to negotiate a sensor nodes across stations, alike it actually detects the sensor nodes that is present in the surveillance surrounded by channels. The negative data insertion, a cooperating inbuilt node can open different types of attacks. In this network model may cause fake negatives, i.e., events that perform occurs without description of source that stands to create the fake reports for valid crisis or packet drain justifies the description of message that is transient.

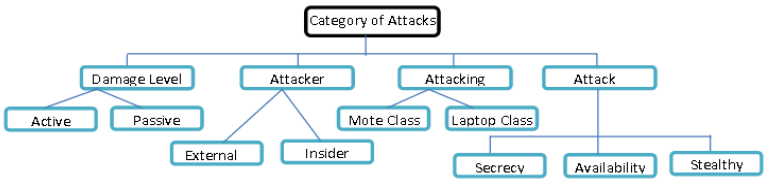


Fig.1: Threat Model.

WSNs is presented by features such as the break level caused, place, network functionality and attacker's strength

Section each of these is explained with respect to the function and effect of the attacks. Figure 1 shows the threat model that has been used in this paper to evaluate various attacks and effects of these attacks on the network

B. *HOP-BY-HOP AUTHENTICATION*

The interleave hop-by-hop verification types illustrate the theory about wireless sensor networks described below,

- The mobile ado networks first initializes the consumption part, a slave performs whole mobile networks with a characteristic identity, such that accessories are equipped to permit the node to establish pair-wise keys with other nodes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

- An association discovery node classifies the mobile identity of its linked nodes. The model process is proposed by the compromised nodes occasionally, so that the sensor nodes will find the collapse that is occurring in the nearest node.
- The testimony advocacy section of protuberance will spawn a collective node, so that it exposes the number of occurrence of crisis for attention.
- The en-route sorting phase, each promoting mobile nodes validates the MAC calculates the minor related nodes that eliminate MAC from the destination.
- The source station guarantee phase (BS) validates the report after message in receipt of it. The BS notices the Nodes that is incremented and agrees the nodes that have proper description. After that it obtains the result or else it dispenses the result.

C. *SECURE KEY DISTRIBUTION MODEL*

The secure key distribution model shares some of the related details about the mobile ado networks, so it merge links in any time to protect the key, it ensures a faithful online resource at the beginning. The scheme is n level secure of n users, grouping jointly their parts and none of the details about the keys will be known. This process will be additionally divided in to two groups. (i) Integrative (The owners occupies a procedure preceding the management of frequent keys) and (ii) non-integrative (The keys are engendered confidentially to the person).

D. *TIMED EFFICIENT STREAM LOSS TOLERANT AUTHENTICATION (TESLA)*

The model uses mainly single cryptography mechanisms, and uses particular time delayed key discovery to attain the required irregularity property. However, the stream loss model needs insecurely coordinated clocks between the source and the destination. It provides packet deferred per data verification and dependability examination. The main idea is focus to given that both competence and security is a delayed discovery of keys. The delayed key disclosure results [4] in a validation delay. In performs the delay is on the order of RTT (round-trip-time).

The following properties are described below:

- Short calculation is overhead for production and verification information.
- Partial buffering for the source and the destination each individual packet.
- Strong truthfulness to packet errors.
- Different dimensions to a huge number of receivers.
- Keeps the receivers from denial of service attacks (Dos) in those situations if configured properly.
- Every receiver does not verify packets authenticity unless it is loosely timely synchronized with the sender, where synchronization can take place at meeting setup.
- Non denial is not supported with each receiver can know about a packet stream is from valid source, but cannot prove this to a third party.

The model is used in network layer, the transport layer, or the application layer. Late verification, however, requires buffering of packets receiving until authentication is completed.

E. *ENCRYPTION AND DECRYPTION METHODS*

The message verification is used to follow the Encipher and decipher mechanisms. To encipher a text, it verifies methods with a encipher key (e and n) is followed. To indicate the text as values between zeroes and n minus 1.

For enciphering the text just lift the e mod n. As a result the cipher text is denoted as C will be the remainder of the text that separates n values.

For deciphering the text, just lift an alternate values d, such that d mod n. The encipher and decipher algorithms are:

$$C \equiv E(MSG) \equiv MSG^{e} \text{ modulo } n, \text{ for a Text}$$
$$D(C) \equiv C^{d} \text{ modulo } n, \text{ for a coherent of text.}$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

The enciphered key is thus a pair for real values of encryption. Equally the deciphered key is thus a combination of real values. Every individuals compose their public enciphered values and have their respective deciphered key as unique.

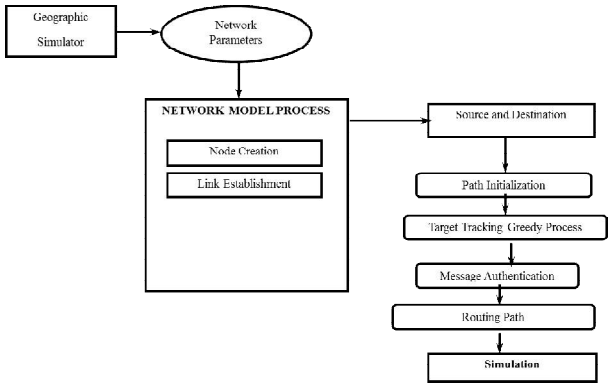
III.ALGORITHM: ENCRYPT AND DECRYPT

Step 1: The encipherment value e is the binate portrayal.
Step 2: Put cipher text value as real.
Step 3: for $i = n, n \ldots 0$:
Put C is rest of squares of C when spitted by integer.
Step 4: Stop. Currently C is the enciphered form of text.

IV.PROPOSED METHODOLOGY

Message Authentication is one of the most competent results to prevent unconstitutional and depraved messages that are being delivered indoors of wireless sensor networks. Because of this peculiar reason, many message authentication schemes gets matured, depends on either symmetric or public key techniques. The Wireless sensor networks facilitate the compilation and investigation of data from various stations. The proposed method of secure message Authentication by target tracking greedy search method(TTGM) afford feasible remedies that alleviate susceptibility diagnose in the formal risk assessment. The counterfeit of new methods confess the actual cost of attaining a target. The proposed system can allow the intermediate node authentication in a secure way.

V.ARCHITECTURE DIAGRAM



ALGORITHM USED

Greedy distributed sparse spanning tree routing

VI.GREEDY SEARCH MECHANISM

The Greedy mechanism is an adequate, sectarian ado routing scheme hired in many current geographic routing algorithms. By Greedy Mechanism a node makes routing arrangement depends on the areas of one of its neighbors, therefore by restricting the aerial of cultivating several geographical information's. In each steps, always the nodes will deliver the packet to the nearest node with precise length to reach the terminal. Therefore a substitute forwarding scheme prefers the nearest node with shortest distance to reach the terminal by a straight line joining the current node and the terminal .Then the routing node will confront a routing void that is not possible to get closer to reach the terminal. In this case, the routing node prerequisite the packet or penetrate a high complicated resumption mode to

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

route the packet across the routing void. The proposed system proves Greedy mechanisms consistently achieve in sensing the covered networks for dual spectrum property is convinced.

Probably there are four phases evolved in our scheme:

A.NETWORK NODE DISTRIBUTION

In the first phase of our scheme, the mobile nodes are described either in statistically or dynamically to engage crosswise the network, then the nodes are set in the x, y, z direction which has explicit transportation across all the nodes. Simulation areas are based on the number of node creation respectively. In a network the spectrum range of all the individual nodes and dual nodes can broadcast only if they are in the particular range. Then the random nodes are combined in a cubic spare to assure the topologies that are engendered and associated by discharging the nodes that cannot connect and replay the process till the prescribed number of nodes is attained.

B.KEY DISTRIBUTION

In the second phase of our scheme, it has to be implemented once. Every node has to be reloaded along a definite seed key. From the seed key, it can develop a progression of authentication keys using a simple hash function. Then every authentication keys model a hash chain. Among n number of cluster nodes, we consider that there are at least one distinct key for each nodes. If the nodes are negotiated to be active till now, then the intruder will provide access that permit newly broadcast keys. The sender maintains the integrity of the receiver secret. They devise a mechanism for collective data report generation, enrol report, filtering and sink verification.

C. IMPROVED PATH AUTHENTICATION

In the third phase of our scheme, every promoter of the routing path should have the capability to certify the credibility and purity of message. This is achieved by substantiation of public key. Acknowledgment is given to the preceding node if the authentication is successful. A path authentication key exchange mechanism is based on the Diffie Hellman key exchange algorithm, the origin node encrypts the data but a private key is necessary to decrypt the data. The acceptor requests the server to provide a private key. Then the server authenticates the key through the acceptor. Finally it is too difficult to receive the key from the key server for harmful nodes.

D. TARGET TRACKING GREEDY COMPROMISED NODE DETECTION PROCESS.

In the fourth phase which is the final phase of our scheme, the target greedy tracking detection in sensing the nodes, the efficiency and transmission of searching method includes node deployment. This approach has been figure out to formulate the network, and the way of sensing the key distribution and the process of broadcasting the results to the base station. The compromised nodes will spread n number of messages, it obtain some of the possible compromised nodes as a small set.

VII. CONCLUSION

This paper is discussed with different dimensions of hop-by-hop WSN's security have been analyzed. A wide variety of WSNs' attacks at various methods and their classification based on type of attack and security classes have been discussed. In order to secure your communication message authentication in very important. Through proper message authentication only one can achieve great security.

VIII. FUTURE WORK

In future work, we intend to enhance the methodology in Securing Source Privacy in WSN by dynamic path activation based on message Authentication to develop experimental methods for distributed network to control the growth of path of the result data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in IEEE INFOCOM, March 2004.
[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.
[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486
[4] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in IEEE Symposium on Security and Privacy, May 2000.
[5] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.