RESEARCH ARTICLE OPEN ACCESS

Providing High Privacy and Hop-by-Hop Message Authentication in Wireless Sensor Networks

Kudumula Manasa [1], Vadlamudi Muniraju Naidu [2]
M.Tech [1], Associate Professor [2]
Department of Computer Science and Engineering
Narayana Engineering College
Nellore
Andhra Pradesh –India.

ABSTRACT

Message authentication is one of the most effective solutions to thwart unauthorized as well as corrupted messages via being forwarded inside wireless sensor networks (WSNs). For this particular reason, many message authentication schemes have been developed, based about either symmetric-key cryptosystems as well as public-key cryptosystems. Many, however, have the disadvantages of high computational as well as communication overhead as well as need of scalability as well as resilience to node skimp attacks. To address these issues, a polynomial-based scheme was recently introduced. In proposed system concentrates on providing high privacy to the message authentication. In addition to hop-by-hop message authentication key exchange mechanism is enable through deffiee helmen key exchange algorithm the source node encrypts the data after receiver the data it needs a private key for decrypting the data. So the receiver request key server to produce a private key. The key server authenticates the receiver access through key authentication. It is very hard for malicious node to get a key from key server.

Keywords:- Providing Privacy, Hop-By-Hop, Message Authentication, Wireless Sensor Networks.

I. INTRODUCTION

Message authentication is among the most effective solutions to thwart unauthorized in addition to corrupted messages from being forwarded with wireless sensor communities (WSNs). For this particular reason, many authentication schemes are proposed in literature to supply message authenticity in addition to integrity verification intended for wireless sensor communities (WSNs) [1]–[5]. These schemes can largely be divided in two categories: public-key centered approaches and symmetric-key centered approaches.

The symmetric-key centered approach necessitates amalgamated key management, lacks of scalability, and is definitely not flexible to many node compromise attacks because message sender plus the receiver have to share with you a secret essential. The shared essential is handled from the sender to produce a message authentication code (MAC) for every transmitted message. Nonetheless, for this process the authenticity and integrity of the message can simply be confirmed from the node with your shared secret essential, which is typically shared by a gaggle of sensor nodes. An intruder can compromise the real key by incarcerating 1 sensor node. Moreover, this method is not useful in multicast communities. For the public-key centered method, each message is transmitted along with the digital signature of the message produced using the sender's private essential. Every intermediate forwarder plus the final receiver may authenticate the message using the sender's public essential [6], [7]. One of the restrictions of the public key based method could be the high computational cost.

Threat Model and Assumptions:

The wireless sensor communities are implicit to be able to consist of a ton of sensor nodes. The assumption is that each sensor node understands its relative location from the sensor domain and is competent of communicating featuring a neighbouring nodes specifically using geographic course-plotting. The entire system is fully attached through multi-hop marketing communications. It is assumed that there is a security server (SS) which is liable for era, storage and distribution of the security parameters one of the network. This server will in no way be compromised. Nonetheless, after deployment, the sensor nodes could be compromised and seized by attackers. The moment compromised, all data stored from the sensor nodes can be acquired by the opponents. The compromised nodes might be reprogrammed and completely managed from the attackers.

To resolve the scalability difficulty, a secret polynomial centered message authentication plan was introduced with [3]. The ideaof this scheme is related to a threshold magic formula sharing, where the threshold relies on the degree of the polynomial. This approach delivers information-theoretic security of the shared secret key when the quantity of messages transmitted is under the threshold. The intermediate nodes authenticate the authenticity of the message through a new polynomial evaluation. Nonetheless, when the volume of messages transmitted is bigger than the threshold, the polynomial might be fully recovered plus the system is totally broken. An alternative solution was proposed with [4] to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is usually to add a randomly noise, also known as a perturbation factor, to the polynomial so the coefficients of the polynomial can't be easily solved. None the less, a recent study demonstrates the random noise might be completely removed from the polynomial using error-correcting signal techniques [6]. To the public-key based technique, each message is transmitted along with the digital signature of the message generated using the sender's private essential. Every intermediate forwarder plus the final receiver may authenticate the message using the sender's public essential [7], [8]. One of the limitations of your publickey based scheme could be the high computational cost. The recent advance on elliptic contour cryptography (ECC) demonstrates the public-key schemes might be more advantageous with regards to computational complexity, recollection usage, and safety measures resilience, since public-key based approaches possess a simple and clean key management [9].

In this particular paper, we propose the unconditionally secure in addition to efficient source unknown message authentication (SAMA)scheme based on the optimal modified ElGamal signature(MES) plan on elliptic curves. This MES plan is secure against adaptive chosen-message attacks from the random oracle design [10].

However, the compromised nodes will struggle to produce new public keys that could be accepted by the SS along with other nodes. Two forms of possible attacks launched from the adversaries are:

• ***Passive attacks:*** By passive attacks, the adversaries can snoop on messages transmitted from the network and do traffic analysis.

• *Active attacks:* Active attacks may only be commenced from the compromised sensor nodes. In the event the sensor nodes are generally compromised, the adversaries will gain every one of the data stored from the compromised nodes, such as security.Parameters of the compromised nodes. The adversaries can transform the contents of the messages, and introduce their very own messages. An authentication protocol need to be resistant to node skimp on by allowing protected key management. The protocol may provide an integrated key-rotation mechanism or allow for key rotation by an external component.

II. LITERATURE REVIEW

2.1 Wireless sensor networks

Cellular sensor networks simplify the compilation in addition to scrutiny of details from multiple spots [8]. The term wifi sensor network (WSN) illustrates a connection among miniaturized embedded communication devices which supervise and assess their surrounding natural environment. The network comprises many minute nodes sometimes known as motes [5]. A node consists of the sensor(s), your microcontroller, the airwaves communication component, as well as a power source. Wireless sensor nodes range in dimensions from a handful of millimetres to how big is a handheld computer system. Apart from connected with size, sensor nodes reveal general constraints.

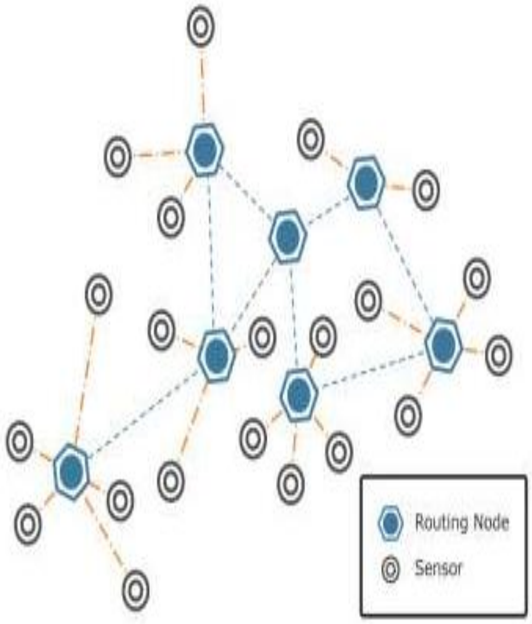

Figure:1.1: wireless sensor network environment.

Security risks with wireless sensor communities contain threats towards the confidentiality, integrity, as well as a availability of the machine. Security methods used on the internet are not merely adaptable to sensor networks as a result of limited resources of the sensors and your ad-hoc feature of the networks. In this particular paper we propose to her Hop by get message authentication through the use of RC6 algorithm.a couple of.

2. 2. NS-2

NS (Version-2) can be an object oriented, individually distinct event simulator. It had been written in C++ with OTcl use while afront-end [10]. The simulator can handle a class pecking order in C++ (compiled hierarchy) as well as a similar class hierarchy inside the OTcl interpreter (interpreted hierarchy) contain. The two hierarchies are generally closely related together; from the user's point of view, there is a new one-to-one relation in between a class from the interpreted hierarchy and something in the put together hierarchy.

Network simulator uses two languages due to the fact simulator has two different varieties of things it has to do. On 1 side, a detailed simulation of protocols has a systems programming language which could efficiently manipulate bytes, supply headers, implement algorithms that cost large data models [12]. For these tasks run-time speed is essential and turn-around time period (run simulation, come across bug, fix bug, recompile, re-run) is less significant. On the different side, a large component of network research consists of slightly varying guidelines or Configurations or quickly exploring quite a few scenarios [10]-[12].

In these cases, iteration time (change your model and re-run) is more important. Since configuration goes once (at the start of the simulation) [5], runtime of this part of the task is less important. Ns meets even though needs with 2 languages, C++ in addition to OTcl [5]. C++ is fast to run but slow to vary, make it made for detailed protocol setup.

An OTcl goes very slower but might be changed very easily (and interactively), turning it into ideal for simulation construction [10]. ns (via tclcl) provides glue to make objects and variables appear on both languages. The tcl interface can be used in cases wherever small changes from the scenarios are simply implemented. Similarly, the C++ code might be changes when processing of allin on its way packets are done, or when changes from the behavior of your protocol is awaited.

In ns, the advance of their time depends on your timing of events that happen to be maintained by a new scheduler [12]. A meeting is an object from the C++ hierarchy with an unique ID, a scheduled time as well as a pointer to the object that handles the presentation. A scheduler maintains an ordered data structure with the events to end up being executed and fires them alongside, invoking the handler of the event [8]-[10].

III. PROPOSED SYSTEM

Our proposed authentication scheme aims at achieving the following goals:

1.Message authentication:

The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.

2.Hop-by-hop message authentication:

Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception [1].

3.Identity and location privacy:

The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic [3].

4. Efficiency:

The scheme should be efficient in terms of mutually computational and communication overhead [15].

In proposed system concentrates on providing high privacy to the message authentication. In addition to hop-by-hop message authentication key exchange mechanism is enable through deffiee helmen key exchange algorithm the source node encrypts the data after receiver the data it needs a private key for decrypting the data. So the receiver request key server to produce a private key. The key server authenticates the receiver access through key authentication. It is very hard for malicious node to get a key from key server.

IV. ARCHITECTURE

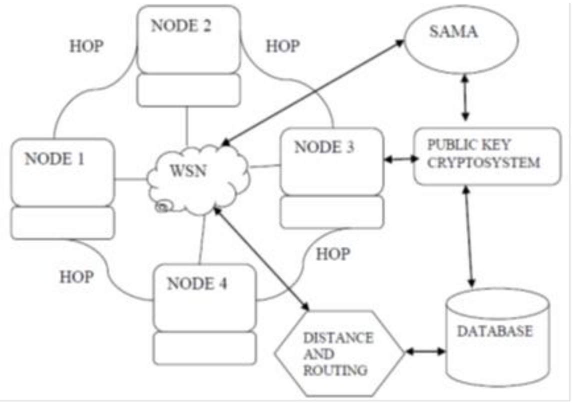

Fig: Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks.

In wireless sensor network provides on high privacy to the message authentication. While enabling intermediate nodes message authentication scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem.

We develop a source anonymous authentication code (SAMAC) an elliptical curve that can be provide unconditional source anonymity through hop-by-hop message authentication process.

V. CONCLUSION

In order to secure your communication message authentication in authentication only one can achieve great plant the proper tree of authenticity. This paper is in order to investigate the different techniques available in message Authentication. In future to develop the a new efficient authentication scheme using the elliptic curve cryptography. In this scheme any node can transmit n number of message without threshold problem. This service is usually provided through the deployment of a secure message authentication code(MAC).

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] W. Zhang, N. Subramanian, and G. Wang, “Lightweight and compromise resilient message authentication in sensor networks,” in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[5] 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.

[6] D. Point cheval and J. Stern, “Security proofs for signature schemes,” in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[7] D. Chaum, “Untraceable electronic mail, return addresses, and digital Pseudonyms,” Communications of the ACM, vol. 24, no. 2, pp. 84–88, February 1981.

[8]. Harsh Kumar Verma, Ravindra Kumar Singh, —Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms‖, International Journal of Computer Applications (0975 – 8887) Volume 42–No.16, March 2012, pp 1-7.

[10]. Raymond Sbrusch, —Authenticated Messaging In Wireless Sensor Networks Used For Surveillance‖, Thesis, The University Of Houston-Clear Lake, May, 2008.

AUTHORS

Kudumula Manasa has received her B.Tech in Computer Science and Engineering from Sri Raghavendra Institute Of Science & Technology, Vinjamur affiliated to JNTU, Anantapur in 2013 and pursuing M.Tech degree in Computer Science and Engineering in Narayana Engineering College (NEC), Nellore, A.P affiliated to JNTU, Anatapur in (2013-2015).

Vadlamudi Muniraju Naidu has received his B.Tech in Computer Science and Engineering from SVCET Chittoor, JNTUH, 2005 and M.Tech degree in Computer science and Engineering from Nagarjuna University in 2010. He is dedicated to teaching field from the last 9 years. He has guided 4 P.G and 10 batches U.G students. His research areas included Networks. At present he is working as Associate Professor in Narayana Engineering College, Nellore, Andhra Pradesh, India.