ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Hop-by-Hop Message Authentication Based on Block Cipher Approach in Wireless Sensor Networks

[I]Srishaila Patil.B, [II]Manjunath.C.R
[I]PG Research Scholar, Jain University, Bangalore, India
[II]Research Scholar, Dept of CSE, Jain University, Bangalore, India

Abstract
In hop by hop message authentication with source security in wireless sensor networks, were verification is successful approach to protect from unapproved clients effected messages from being send through in wireless sensor systems. Numerous message authentication plans have been utilized to secure messages but these authentication plans have the limitations of high overhead, absence of capacity, to node attacks and edge issue. The proposed plan permits any node to transmit an unlimited number of messages without suffering the threshold issue and provide hop-by-hop authentication to the block of data by generating authentication keys and signature. In addition, can also provide message source security. Both theoretical investigation and simulation results exhibit that our proposed plan is efficient than the polynomial-based approach in terms of both computational and communication overhead under practically identical security levels while giving message source protection.

Keywords
Message authentication, hop-by-hop, Wireless sensor networks, signature keys, Message authentication code.

I. Introduction

Message authentication plays an vital part in thwarting unauthorized and tainted messages from being sent in wireless sensor networks to spare the valuable sensor energy. Therefore, numerous authentication plans have been proposed in literature to give message authenticity and trustworthiness check for wireless sensor systems (WSNs). but, the greater part of them have the restrictions of high computational and communication overhead, in addition to absence of scalability and strength to node compromise attacks. To address these issues, a polynomial-based plan was presented. This plan and its expansions all have weakness of a built-in threshold controlled by the level of the polynomial.

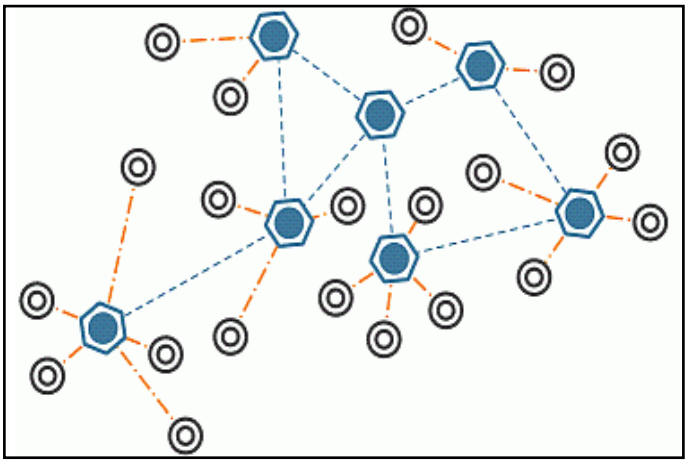

Fig.1 : Wireless sensor networks

The symmetric-key based methodology requires composite key administration, absences of scalability, and is not flexible to extensive quantities of node compromise attacks since message sender and the recipient need to share a secret key.
The common key is taken care of by the sender to create a message authentication code (MAC) for each transmitted message. Then again, for this procedure authenticity and integrity of the message must be affirmed by the node with the mutual secret key, which is normally shared by a gathering of sensor nodes. An intruder can trade off the key by incarcerating a sensor node. Likewise, this system is not valuable in multicast networks. For the general public-key based strategy, every message is transmitted along with the digital mark (signature) of the message delivered utilizing the sender's private key. Every intermediate forwarder and the last recipient can authenticate the message utilizing the sender's public key .One of the restrictions of public key based strategy is the high computational overhead.

A. Motivation

In wireless sensor systems security assumes a critical part, subsequent to sending the information from the source node to the destination it will reach productively and there is no loss of information, In our proposed framework after the information transmitted from source it will transfers to the intermediate hop and provide hop-by-hop authentication to the data and forwards to the destination and if there is malicious hop, information will be lost and in non-malicious hop information will be authenticated and forwards to the destination.

B. Scope of the Project

This project focuses on enhancing on improving the functionalities in Wireless sensor networks(WSN's), which as of now exists however is upgraded by Hop-by-hop Message authentication in WSN's, This usefulness gives authentication to the Block of data exchanging from source to the destination without loss and less energy consumption and block of data exchanges through the node to achieve the destination.

C. Proposed System

Our proposed Authentication plan goes for accomplishing the following objectives:

- Message verification: The message beneficiary ought to have the capacity to check whether a got message is sent by the hub that is guaranteed or by a hub in a specific gathering. As it were, the adversaries can't pretend to be a honest hub and infuse fake messages into the system without being detected.
- Hop-by-hop message authentication: Every forwarder on the directing way should have the capacity to check the authenticity and integrity of the messages upon reception..
- Identity and location privacy: The adversaries can't focus the

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

message sender's ID and area

- Efficiency: The plan ought to be effective as far as both computational and communication overhead.

II. Techniques

Various message authentication schemes have been created, in perspective of either symmetric-key cryptosystems or public key cryptosystems. A large portion of them, regardless, have the confinements of high computational and communication overhead .furthermore absence of strength and quality to node compromise attacks,, validation arrangement taking into account elliptic curve cryptography (ECC) There were distinctive schedules have been made to explain the issue, for instance, symmetric key cryptography and public key cryptography. Each would have their own issues, with a particular deciding objective to deal with such issue we developed another validation arrangement using the elliptic curve cryptography. In this arrangement any node can transmit n number of message unbounded issues. One of the restrictions of the public key based plan is the high computational overhead. Therecent progress on elliptic curve cryptography (ECC) demonstrates that public key plans can be more significant regarding computational many-sided quality, memory utilization, and security flexibility, since public key based procedures have a straight forward and clean key management. Using the Message Process 5 (MD5) and Secure Hash Calculation 1 (SHA-1) verification schedules characterize RFC 5880, the BFD Single hop security elements gives security against assaults on data connections between two or specifically joined gadgets included in a BFD session

III. System Design

The proposed architecture mainly focuses hop-by-hop message authentication in the wireless sensor systems, Block of information from the source exchanges through the intermediate sensor nodes and this encrypted information will be validated by the hops using authentication keys and signature, from the hacker hops and finally achieve the destination hop without the loss of the information. The sensor hops will check the block of encoded information while exchanging from source to the destination by detecting the attacker node in the wireless sensor systems.

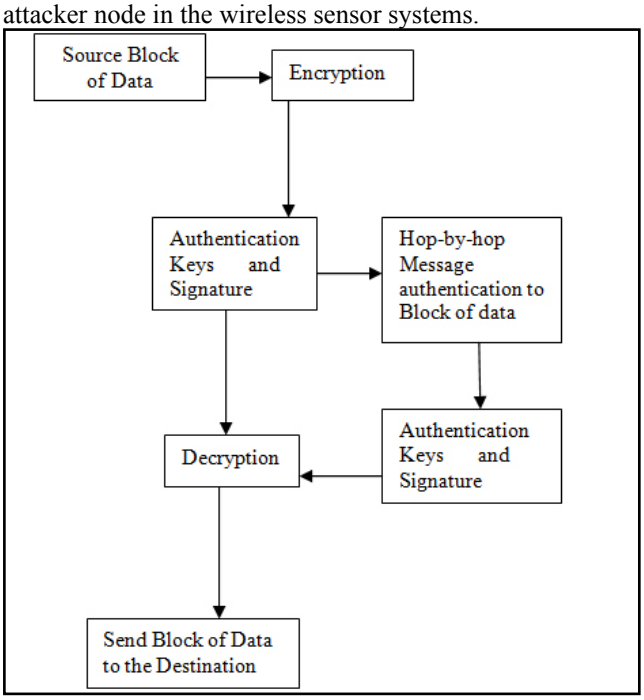

Fig.2: System Overview

IV. Simulation Setup

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the test system somewhat on account of the scope of components it provides and partly because it has an open source code that can be modified and extended.. There are distinctive renditions of NS and the most recent variant is ns-2.1b9a while ns-2.1b10 is being worked on, Network simulator (NS) is an object–oriented, discrete occasion test system for systems administration research. NS gives significant support to detailed protocol implementation of TCP, steering and multicast conventions over wired and wireless systems. The test system is an aftereffect of a progressing exertion of examination and created. Despite the fact that there is a significant trust in NS.NS is composed in C++, with an OTcl1 mediator as an order and arrangement interface. The C++ part, which is quick to run yet slower to change, is utilized for point by point convention execution. The OTcl part, then again, which runs much slower however can be changed quick rapidly, is utilized for detailed protocol implementation guarantees that the whole incorporated programming framework meets necessities. It tests a setup to guarantee known and predictable results. A sample of framework testing is the design situated framework integration. In Wireless Sensor Networks Message Authentication assumes an imperative part while exchanging the information from the source to the destination through intermediate nodes But while while exchanging of information from source to the destination there is no certification of complete conveyance of information to the destination, Because of authentication issue in every hope in the wireless sensor systems.

In our prosed system after executing the tcl file simulation of hop-by-hop message authentication starts with sending block of data from source to the destination, tool command line is an front end scripting language used and c++ as the backend programming language used in our proposed system. Initialize the nodes in the wireless sensor networks the source node provide authentication to the block of data and forwards to the next hop only when signature and authentication keys match. Every single second simulation details will be recorded in the trace file.so that can able to check the each node functionality after the simulation in the trace file. After the complete simulation of the hop-by-hop message authentication separate awk files are created for energy consumption of the node, average packet delivery ratio, average packet loss ratio and end- to end delay between the nodes. Received hop provide authentication from misfortune and defilement to the block of data and finds next hop confirmation and signature keys to coordinate. NS is composed in C++, with an OTcl1 mediator as an order and arrangement interface. The C++ part, which is quick to run yet slower to change, is utilized for point by point convention execution. The OTcl part, then again, which runs much slower however can be changed quick rapidly, is utilized for detailed protocol implementation guarantees that the whole incorporated programming framework meets necessities.

Every forwarder on the directing way should have the capacity to check the authenticity and integrity of the messages upon reception. This usefulness gives verification to the Block of data exchanging from source to the destination without loss and less energy consumption and block of data exchanges through the node to achieve the destination. authenticity and integrity of the message must be affirmed by the node with the mutual secret key, which is normally shared by a gathering of sensor nodes.

V. Results and Discussions

In our proposed framework, Authentication is given to each

hop(hop-by-hop) for forwarding block of data in wireless sensor systems. At first block of data sending from source to the destination through hop-by-hops in the wireless sensor systems. Source node creates the authentication keys and signature in the WSN's, information from the source node finds the most efficient shortest way using prim's algorithm to reach the destination. every hop produces the authentication keys and signature, if both source node and next hop matches with authentication and signature keys then source sends the data to the next hop. Received hop provide authentication from misfortune and defilement to the block of data and finds next hop confirmation and signature keys to coordinate. All simulation will be recorded in the trace file by every second in trace file each simulation action will be recorded.

Table 1 : Results discussions

Description	Action	Expected Results
Source	Provide authentication to block of data and generate sig keys	Forwards authenticated block of data to destination
Hop-by-hop	Signature keys generate and provide authentication to received block of data	Authenticated block of data sends to the next hop
Provide authentication	Hop-by-hop authentication to block of data	Authenticated data forwards to the destination
Destination	Final authentication key generated to receive block of data	Receives data successfully, without loss

VI. Conclusion

Here the concluded information is the proposed efficient source intermediate hop-by-hop node message authentication scheme based on signature and ID generation provides high security than the other methods in the existing research and order to investigate the different techniques available in message Authentication. The excepting results is, our proposed scheme is efficient than the polynomial- based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption. While ensuring message sender privacy, this scheme can be applied to any message to provide message content authenticity. In future to develop a new efficient authentication scheme using different techniques. 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.

References

[1] *Jian Li Yun Li Jian Ren Jie Wu, "Hop-by-Hop Message Authentication and Source privacy in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems,Volume:25,Issue:5,Issue Date : May.2014*

[2] *Prof N.R.Wankhade, Jadhav Ashvini B. "A Survey Paper on Hop by Hop Message Authentication in Wireless Sensor Network", N.R.Wankhade et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014*

[3] *Sonam Bais a, Prof. Animesh Tayal,"An Overview on Message Authentication in Wireless Sensor Networks Based on Analysis of Block Cipher Algorithm," International Journal on Recent and Innovation Trends in Computing and Communication may 2014*

[4] *Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho,"An improved RC6 algorithm with the same structure of encryption and decryption ", Birla Institute of technology and science. conference on March 03,2010*

[5] *Nikodin Ristanovic1, Panos Papadimitratos, "Adaptive Message Authentication for Multi-Hop Networks", 2011 Eighth International Conference on Wireless On-Demand Network Systems and Services*

[6] *Dipika.R.Bisne1,Mr..Punesh.U.Tembhare," Review on Design and Implementation of Hop toHop Message Authentication and Source Privacy in Wireless Sensor Networks ", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2015*

[7] *Md Imran alam,Mohammed Rafeek khan"Performance and efficiency analysis of different Block cipher algoriths of symmetric key cryptography" Volume 3, Issue 10, October 2013*

[8] *Shital Y.Gaikwad,U.V.Kulkarni "Comparative Analysis of Hop-to-Hop and End-to-End Secure Communication"*

[9] *Shital Y.Gaikwad,U.V.Kulkarni "Comparative Analysis of Hop-to-Hop and End-to-End Secure Communication" IEEE Transactions on Parallel and Distributed Systems,Volume:25Issue:2,Issue Date:Feb.2014*

[10] *Usham Robinchandra Singh, Sudipta Roy, Herojit Mutum "A Survey on Wireless Sensor Network Security and its Countermeasures: An Overview" International Journal of Engineering Science www.ijesi.org Volume 2 Issue 9September.*

[11] *S.Chaitanya Rami Reddy, P.Ravinder Kumar "Implementation of Data Aggregation and Authentication in Wireless Sensor Networks" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5, November 2012*

Author's Profile

Srishaila Patil.B. Dept.of computer science and engeneering PG Research Scholar, Jain University,Bangalore,India

Manjunath.C.R Asst. Professor, Dept.of computer science and engeneering Jain University Bangalore, India. Has published more than twenty plus research publication in various reputed journals and supervised twenty plus research scholars.