IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Reliable Hop-by-Hop Message Validation in Wireless Sensor Network using Cryptography based Network Model

Navyatha K P[1], **Mrs. Sahanadevi K J**[2]

M.Tech Scholar, Dept. of CSE, East West Institute of Technology, Bangalore, India[1]

Asst. Professor, Dept. of CSE, East West Institute of Technology, Bangalore, India[2]

Abstract: Message validation is one of the effective ways to thwart the threat of unauthenticated and unwanted messages that are communicated through Wireless Sensor Network (WSN). To overcome this problem, many workers have proposed various models using different techniques like key based cryptosystems using symmetric key or public key cryptosystem. However, most of these mechanisms have limitations due to their high computational and communication overhead, in addition to scalability problem and threat of node compromise. To address these challenges researchers introduced polynomial-based model, though these models also have inherited weakness of the polynomial. To provide a more robust and effective security measure, we are proposing a scalable validation mechanism based on the security model (SM). The proposed system permits any node to transmit unrestricted number of data without undergoing the threshold problem. Further the proposal enables message source privacy. Through simulation trails, it is proved that this system is more efficient than the polynomial based model in terms of computational and communication overhead under similar security stages with additional message source privacy.

Keywords: Cryptography, dataintegrity, Message validation, source privacy, WSN.

I. INTRODUCTION

The wireless communication, sensor technology, and embedded computation technology have advanced the rise and development of Wireless sensor Network (WSN). WSN comprises of countless miniaturized scale sensor nodes deployed in the observation region, which is a multi-hop self-organizing network system shaped by wireless communication technique to sense, gather, and process the data detected by sensors in the system distributed zone and after that forward the outcomes to its users [1].

Of late, WSN as developing system advancements is finding lot of applications in various fields since they provide considerably measureable, detailed and dependable data in the system distributed region at whatever time and place. Because of these merits, the WSN extensively used in military resistance, industry, agriculture, development and urban administration, biomedical and ecological monitoring, emergency services, public security and antiterrorism, unsafe and destructive regional remote control, etc. All these fields are tremendously accounted by several government bodies. Hence, WSN has a significant scientific and practical importance [2].

Although WSN are deployed in rough situations like regions with less human access or in enemy region. However, the system has its own limitations in its energy, data processing, storage capacity and bandwidth. Further, different factors of remote system are restricted, which makes WSN defenseless against attacks. The security of WSN is of incredible social concern especially in some critical regions, (for example, military target discovery and tracking) because once the sensor system is under attack or damaged, this would likely prompt tragic results.

Sensor systems pose security challenges due to their inherited constrains in communication and processing. The nature of sensor systems deployment makes them more vulnerable to different attacks. Since the sensor systems are stationed in applications where they have physical interaction with the environment, individuals and different items making them more defenseless against security threats. Characteristic constraints of sensor systems can be classified as node and network constraints. The protection and security issues in sensor systems bring up lot of research challenges. Dense distribution of sensor systems in an unattended domain makes sensor nodes defenseless against potential attacks. Attackers can seize the sensor nodes and trade off the system to acknowledge illegitimate nodes as honest nodes. Once inside the system, attacker can perform various kinds of attacks. Advancement in hardware and software will have to address these issues at some degree. A robust secure sensor systems require deployment of countermeasures, for example, secure key administration, secured routing and light weight encryption methods [3].

Therefore, the best approach to design security techniques can give secrecy assurance and authentication elements to avoid harmful attacks and make a generally safe workplace for sensor systems, to ensure the WSN are realistic. In this way, the issues and difficulties confronted by WSN security technology are turning into the principle research domain everywhere throughout the world.

DOI 10.17148/IJARCCE.2016.5521

In the above context, the present work is organized as follows, Section II provides literature survey. Section III Proposed system along with implementation of the proposed method. Section IV describes the results and discussion of the proposed method. Then, finally the conclusion and also the future research direction has been explain in section V.

II. LITERATURE SURVEY

A perusal of the review of literature on the subject throws light on various works, problems encountered, various techniques used, the resulted solutions and the end result evaluation.

Working on the further validation of Bilinear Diffie-Hellman technique for transport message security provided by vehicles, Huang et al [4], emphasized authenticity of RSU and TAs identity and the effectiveness of key. The authors opined that their work can satisfy source of authentication, message integrity, nonrepudiation, privacy and conditional untraceability requirements. They further stressed that vehicle message should be real time and should not be complicated to validate the message calculation.

Nandu and Shekokar [5] performed a study to accomplish new re-programming protocol that is more secure and quicker while keeping up all the significant elements of re-programming, for example, version control, scope determination, encoding/decoding, code dissemination. When used as framework, high level of security, better calculation and communication execution is reachable in contrast to the traditional system security arrangements.

Reviewing the work done on various aspects of security, Rajeshwari and Seenivasagam [6] felt that a strong and reliable security services are a must to ensure integrity, authenticity and confidentiality of the critical information. In WSNs, broadcast transmission is extensively used along with extensive usage of wireless messages and their applications. Therefore it is critical to authenticate broadcast messages.

Authenticity of information is protected using cryptographic hash functions. However, some of the commonly used hash algorithms require huge computational overhead which is difficult to operate in energy-starved networks like WSN. Working on the above aspects Chowdhury et al [7] have developed a light-weight one-way cryptographic hash algorithm to address the problem of energy starved wireless network. According to them these algorithms fulfills all the basic properties like preimage resistance, collision resistance of a one-way unkeyed hash function.

Debnath et al [8] proposed a ring signature technique to authenticate the source node without altering its spatial privacy. This approach is based on the assumption that the veracity of message from a sensor node must be verified to avoid a false reaction by the sink. They are of the opinion that precaution must be taken to preclude the possibility of a traffic analysis attack by an adversary by considering other nodes like signers and their numbers. The ring signature structure proposed by them requires approximately four individuals from the same neighbor region of the source node to sustain privacy of the node. It was further assured that the small overhead they incorporated did not adversely affect the performance of the sensor network.

Data source location privacy (DSLP) is of at most importance for some asset monitoring applications in WSNs. In general, the source simulation method is commonly used to protect the DSLP against global eavesdropper in various WSN applications. However, these methods are based on panda-hunter game model (PHGM) have not considered the communication between data sources and reporter sources and often leads to its ineffectiveness. The source simulation method has two limitations like it cannot generate effective event reports and also not suitable to track multiobjects accurately. To address these issues Hu et al [9] proposed improved source simulation method to improve event report strategy and an updated panda-hunter game model (UPHGM). According to them, based on UPHGM an energy efficient grid-based pull (GBP) scheme is also designed to protect the DSLP by combining a light-weight security object with an effective grid partition method.

Though many protocols, for sensor network security, provide confidentiality for the content messages in mobile phones the contextual information is still exposed. Such exposed contextual information can be exploited by an adversary to extract sensitive information like locations of the monitored objects and data sinks in the field. Such exposures adversely affect network applications. Further the existing techniques have limited capacity to defend leakage of location information. Therefore a strong global level eavesdropper is required to defeat the existing techniques. Working on these aspects Mehta et al [10] proposed two strategy to give location privacy to monitored object (source-area privacy)- occasional gathering and source reproduction and two strategies to give location security to data sinks (sink-area privacy)- sink simulation and backbone flooding. These procedures give tradeoffs between latency, privacy and communication cost. Further they have shown that their proposed procedure is proficient and powerful for source and sink-area privacy in sensor systems.

III. PROBLEM DESCRIPTION

One of the most efficient and effective ways of thwarting corrupted and unauthorized messages that are forwarded through WSNs can be achieved using message validation mechanism. The message authentication process involves the process of confidential identification of one user by the other user or even the process of identity confirming. Message validation could be used to identify the intruder capable of compromising the nodes and corrupting data in WSN. Due to this fact, large number of message validation mechanisms is proposed using symmetric key cryptosystems or public key cryptosystems.

Message authentication is considered as one of the most efficient techniques which can be applicable for mitigating various issues associated with the traditional symmetric-

DOI 10.17148/IJARCCE.2016.5521

key cryptography and public key cryptography techniques. However, many problems still arise with the existing techniques which are unable to stop the unauthorized and corrupted messages that are being forwarded in WSNs. The present study introduces a polynomial-based technique which can be applicable for mitigating these issues.

IV. PROPOSED METHOD AND IMPLEMENTATION

In the proposed work, we concentrate on planning and building up of an adaptable verification plan which is based on the idea of elliptic bend cryptography (ECC). For empowering the middle nodes check, the proposed framework helps any node to create and convey lots of messages without suffering from any sort of problem or interruptions. The proposed method incorporates financially viable device of secured verification model with the utilization of circular bend cryptography in WSN. In addition to this, the proposed system can also protect the message source.

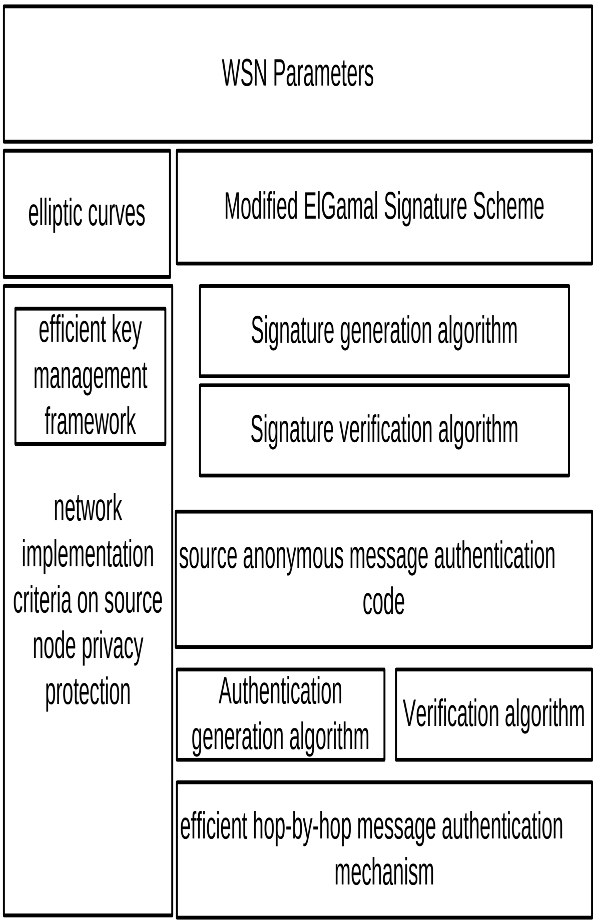

WSN Parameters
elliptic curves
Modified ElGamal Signature Scheme
efficient key management framework
Signature generation algorithm
Signature verification algorithm
network implementation criteria on source node privacy protection
source anonymous message authentication code
Authentication generation algorithm
Verification algorithm
efficient hop-by-hop message authentication mechanism

Fig 1. System Architecture of the Project

The system architecture of the project is explained in fig. 1. This proposal offers a better security protocol that guarantees source node anonymity along with efficient message verification scheme. The system considers the basic usage of elliptical curve which is then subjected to modification that enables the system to authenticate the single process without individually verifying the signatures using Algorithm. The above diagram describes how verification of message is done for pool proof authentication. In this process initially the message is generated by taking random number and this message is validated using modified Elgamal Signal Scheme. However, to make message pool proof, in the present proposal it is validated using the procedure shown in the diagram which is much more stronger and is more trust worthy in finding the message source.

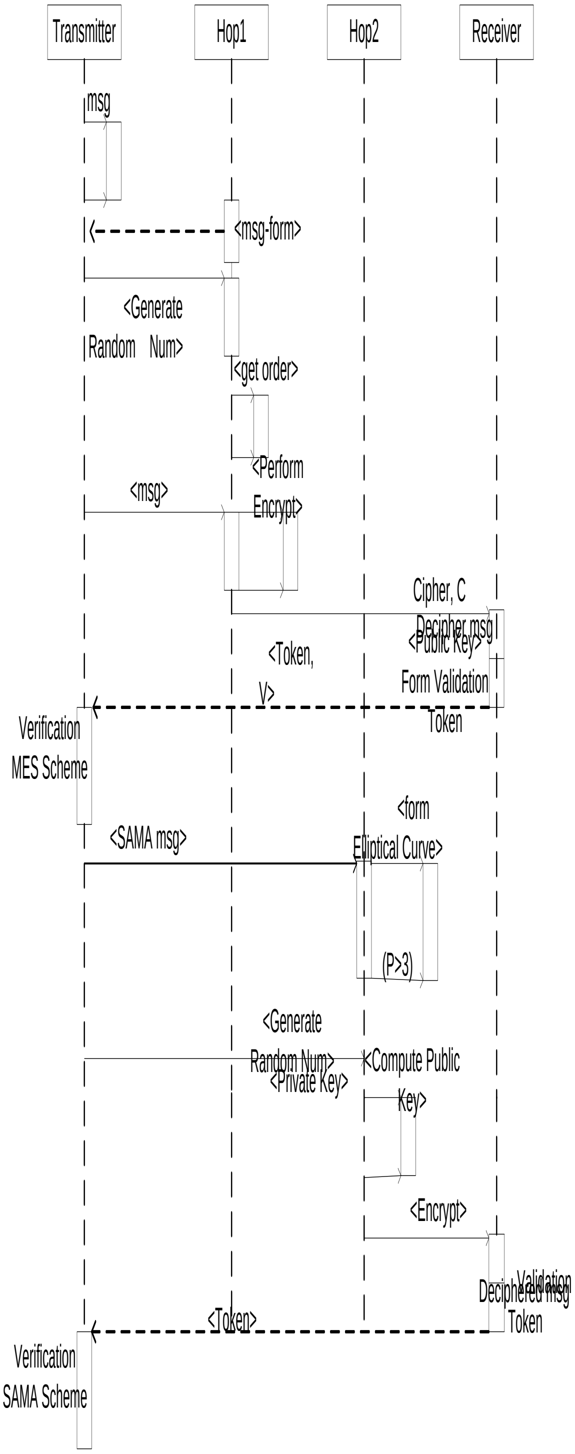
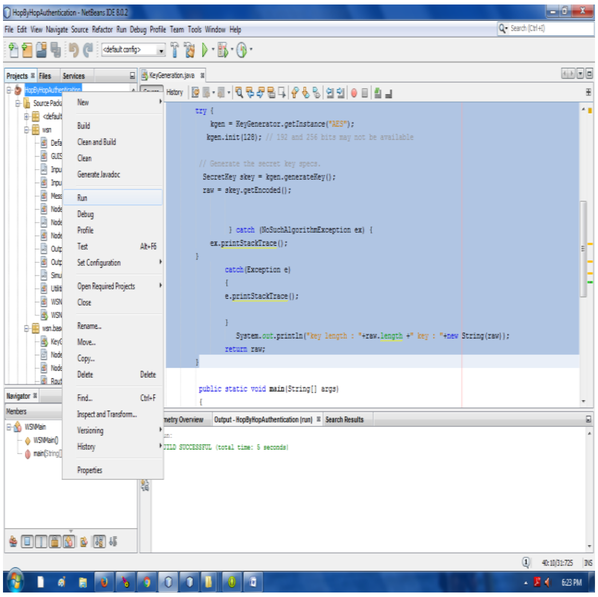


Fig 2. Sequence Diagram of the Proposed System

DOI 10.17148/IJARCCE.2016.5521

V. RESULTS AND DISCUSSION

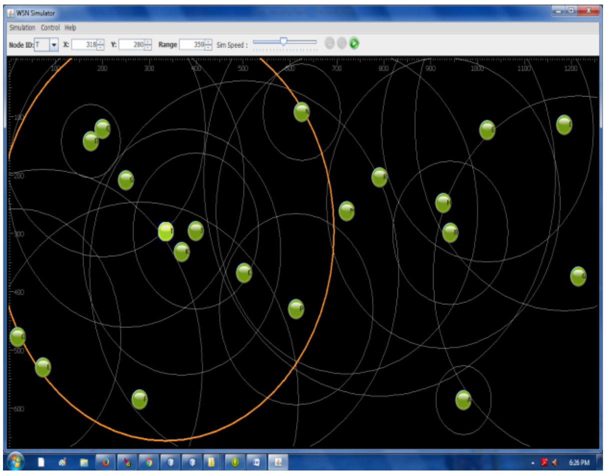
The present proposal to develop a reliable hop-by-hop message validation in WSN using cryptography based network model has been evaluated following standard procedures. The result of the same has been depicted in the form of several screenshots. The details of screenshots include: selection of the message authintication project using NetBeans IDE (figure 3), initializing message transmission communication range in WSNs(figure 4), process of routing in WSN form nodes to base station (figure 5), transferring message from node to node till base station (figure 6), selection of Source and Destination node (figure 7), message transmission from Source and Destination node (figure 8), details of message transmission form source to destination node (figure 9).



```
try {
   kgen = KeyGenerator.getInstance("AES");
  kgen.init(128); // 192 and 256 bits may not be available

 // Generate the secret key specs.
 SecretKey skey = kgen.generateKey();
 raw = skey.getEncoded();


      } catch (NoSuchAlgorithmException ex) {
   ex.printStackTrace();
}
      catch(Exception e)
      {
      e.printStackTrace();

      }
        System.out.println("key length : "+raw.length +" key : "+new String(raw));
      return raw;
}

public static void main(String[] args)
{
```

```
un:
UILD SUCCESSFUL (total time: 5 seconds)
```

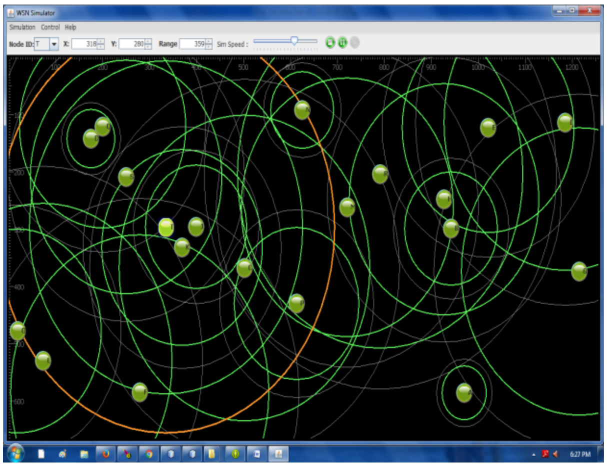
Fig 3. Selection of the message authintication project using NetBeans ID



Node ID: 7 X: 318 Y: 280 Range: 359

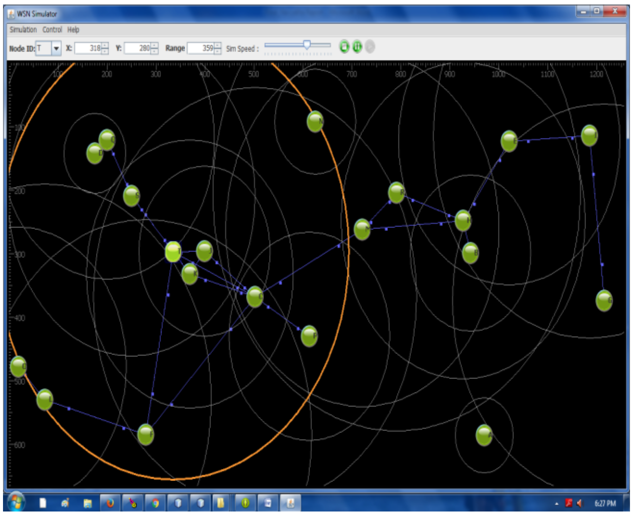
Fig 4. Initializing message transmission communication range in WSNs

The resultant outcome discussed in the form of performance using Net Beans IDE where the step by step implementation of details has been shown in the form of simulations which enabled to arrive at reliable hop-by-hop message validation in WSN using cryptography based network model. The design and evaluation were carried out using the above simulations by adopting the Net Beans IDE.



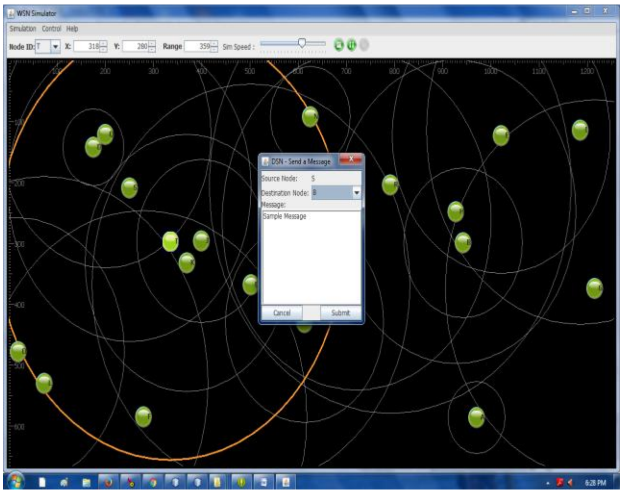
Node ID: 7 X: 318 Y: 280 Range: 359

Fig 5. Process of routing in WSN form nodes to base station



Node ID: 7 X: 318 Y: 280 Range: 359

Fig 6. Transferring message from node to node till base station

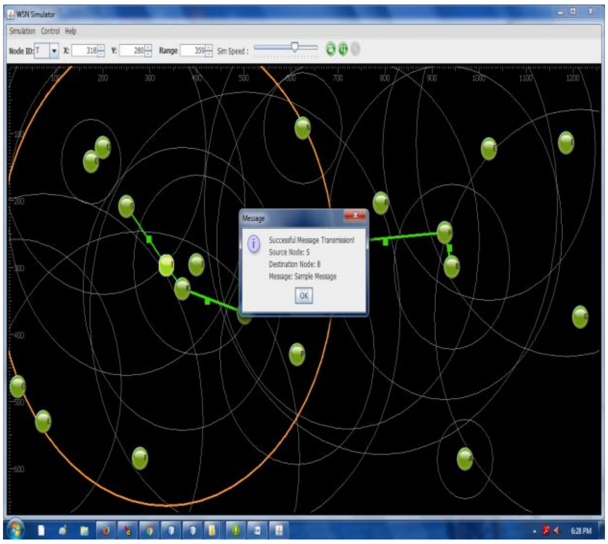


Node ID: 7 X: 318 Y: 280 Range: 359

Source Node: 5
Destination Node: 8
Message:
Sample Message

Fig 7. Selection of Source and Destination node

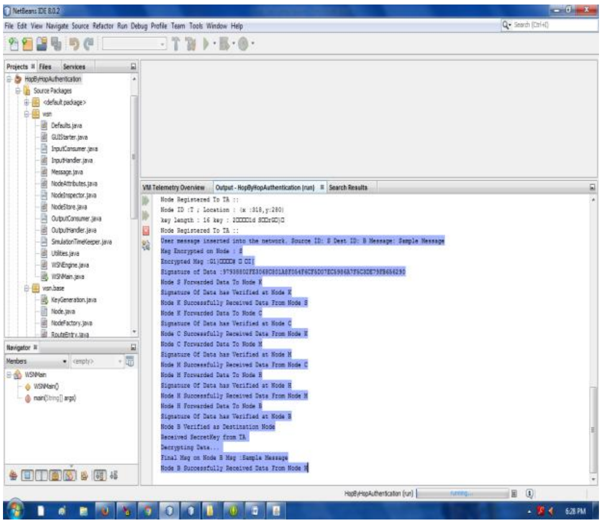
DOI 10.17148/IJARCCE.2016.5521



Node ID: T X: 318 Y: 280 Range: 359

Successful Message Transmission!
Source Node: S
Destination Node: B
Message: Sample Message

Fig 8. Message transmission from Source and Destination node



```
Node Registered To TA ::
Node ID :T ; Location : (x :318,y:280)
key length : 16 key : 2□□□□1d S□□r□□)□
Node Registered To TA ::
User message inserted into the network. Source ID: S Dest ID: B Message: Sample Message
Msg Encrypted on Node : S
Encrypted Msg :01)□□□□# □ □I(
Signature of Data :97938802FE3068C801A8F064F6CF6D07EC5986A7F6C8DE79FB656290
Node S Forwarded Data To Node K
Signature Of Data has Verified at Node K
Node K Successfully Received Data From Node S
Node K Forwarded Data To Node C
Signature Of Data has Verified at Node C
Node C Successfully Received Data From Node K
Node C Forwarded Data To Node M
Signature Of Data has Verified at Node M
Node M Successfully Received Data From Node C
Node M Forwarded Data To Node H
Signature Of Data has Verified at Node H
Node H Successfully Received Data From Node M
Node H Forwarded Data To Node B
Signature Of Data has Verified at Node B
Node B Verified as Destination Node
Received SecretKey from TA
Decrypting Data...
Final Msg on Node B Msg :Sample Message
Node B Successfully Received Data From Node H
```

Fig 9. Details of message transmission form source to destination node.

VI. CONCLUSION AND FUTURE RESEARCH DIRECTION

The proposed technique uses ECC for encryption key generation. SAMA scheme can be applicable to any of the message for confidentiality. The polynomial based scheme also provides hop by hop authentication without issues associated with built in thresholds. The study also introduces a hop by hop authentication scheme which is based on SAMA approach. It can be applied to the WSNs nodes with the fixed sink node. Possible techniques for compromised node identifications also have been discussed in this study. The result analysis shows that the proposed technique has been compared with the bivariate polynomial based scheme. The proposed system is more efficient than any other systems in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

Although several reliable hop-by-hop message validation approach in WSN using cryptography based network model are available. However, a lot has to be done in the field. The software designs and programs developed all over the world get accumulated every day and the approach, methodology, intensions, objectives, targets are overlapping and confusing. So under these circumstances any claim on reliability is not sufficient and there always exist a big vacuum which need to be filled by many consorted efforts.

REFERENCES

[1] Zhou, Guang-Dong, and Ting-Hua Yi. "Recent developments on wireless sensor networks technology for bridge health monitoring." Mathematical Problems in Engineering 2013 (2013).

[2] Q.Yang,X.Zhu.H.Fu and X.Che,"Survey of Security Technologies on Wireless Sensor Networks", Journal of Sensors,Hindawi Publishing Corporation,vol 2015.

[3] Zia, Tanveer, and Albert Zomaya. "Security issues in wireless sensor networks." Systems and Networks Communications, 2006. ICSNC'06. International Conference on. IEEE, 2006.

[4] Huang, Mei-Wen, et al. "Using BDH for the Message Authentication in VANET." Mathematical Problems in Engineering 2014 (2014).

[5] P.Nandu and N.Shekokar, "An Enhanced Authentication Mechanism to secure Re-Programming in WSN", ICACTA-2015, Elsevier, 2015.

[6] S.R.Rajeshwari and V.Seenivasagam,"Comparative study on various Authentication Protocols in Wireless Sensor Networks",The scientific World journal,2015.

[7] A.R.Chowdhury, T.Chatterjee, S.DasBit,"LOCHA: a Light weight one way cryptographic hash algorithm for wireless sensor network",Procedia computer science,Elsevier 2014.

[8] A.Debnath, P.Singaravelu, S.Verma,"Privacy in wireless sensor networks using ring signature",Journal of King Saud University-Computer and Information Sciences,july 2014.

[9] Rong-huaHu, Xiao-meiDong,andDa-lingWang,"Protecting Data Source Location Privacy in Wireless Sensor Networks against a Global Eavesdropper", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks Volume 2014.

[10] Mehta, K.; Donggang Liu; Wright, M., "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," in Mobile Computing, IEEE Transactions on , vol.11, no.2, pp.320-336, Feb. 2012.

[11] ssParimalaThulasiraman, Xubin He, Tony Li Xu,"Frontiers of High Performance Computing and Networking - ISPA 2007 Workshops "Springer Science & Business Media, 14-Aug-2007 - Computers - 536 pages.

[12] AzzedineBoukerche,"Algorithms and Protocols for Wireless Sensor Networks", John Wiley & Sons, 03-Nov-2008 - Technology &Engineering.

[13] Yan Zhang, Jun Zheng, HonglinHu,"Security in Wireless Mesh Networks", CRC Press, 21-Aug-2008 - Computers – 552.

BIOGRAPHIES

Navyatha K P completed the BE Degree in Computer Science and Engineering from Reva Institute of Technology and Management, Bengaluru and currently pursuing M.Tech Degree in Computer Networks Engineering at East West Institute of Technology, Bengaluru.

Sahanadevi K J is currently an Associate professor in the Department of Computer Science and Engineering in East West Institute of Technology. She has completed M.Tech Degree in Computer Science and Engineering and she is having 12 years of experience in the field of teaching. Her area of interest includes data mining and data warehousing.

DOI 10.17148/IJARCCE.2016.5521