Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

An Architectural Framework with Multi-layered Security Paradigm for Wireless Sensor Network

Parvathi. C[1] and Dr. Suresha[2]
[1]Assistant Professor, DBIT, Dept of CSE, Bangalore, Karnataka, India
E-mail: Pvc3119@gmail.com
[2]Professor and HOD, SVCE, Dept of CSE, Bangalore, Karnataka, India
Email: suresha_rec@rediffmail.com

Abstract—**The recent advancement in the field of wireless communication, networking, and sensing technologies provides vast possibilities of various promising technologies towards futuristic applications for both civil society and defense related applications. There are many open research challenges which include issues like heterogeneity of network components, communication standards and constraints of resources. This paper focuses on a wireless sensor network (WSN) to provision a novel framework for security to balance the trade-off between performance and resource utilization. The WSN security vulnerabilities are unique as compared to traditional networks due to its unique characteristics. A multifold crypto-mechanism which authorizes the data packets at every hop of the routing path. The simulation results exhibit the effectiveness of the proposed security mechanism.**

***Index Terms*— WSN, Combined Key, Cryptography, Network Security.**

I. INTRODUCTION

The recent advancement in the field of wireless communication has emerged various promising technologies towards futuristic applications (e.g. Civil society and defense oriented applications both)[1] [2]. Rapid advancement and growth in the field of sensing technology bring more real-time challenges to the tiny sensor devices on limited battery power and processing capacity. However a set of self-configuring sensor nodes are enabled together to perform a real time Radio Frequency (RF) communication for transmitting data packets towards a base station, therefore as a whole it defines a particular system namely wireless sensor networks (WSN) communication [3]. The current research trends highlight that WSNs are prone to cyber security attacks more likely as compared to the wired networks due to its dynamicity and ad-hoc nature. It can be seen that WSNs were not only exploited for routing purpose rather it has also been extended to the end to end communication which also requires multi-abstraction based security layer to maintain the data confidentiality irrespective of unauthorized data access on a communication channel [4][5]. The various security requirements such as data confidentiality, authentication, integrity and availability of efficient resources. To meet various security aspects, cryptography has been highly adopted where authorized data packets are transmitted hop by hop. Various existing research journals highlight that the concept of cryptosystem plays a very crucial role to secure the WSN data communication whereas different cryptography applications which have been introduced till date are classified and highlighted below in figure 1.

Grenze ID: 02.ICCTEST.2017.1.60

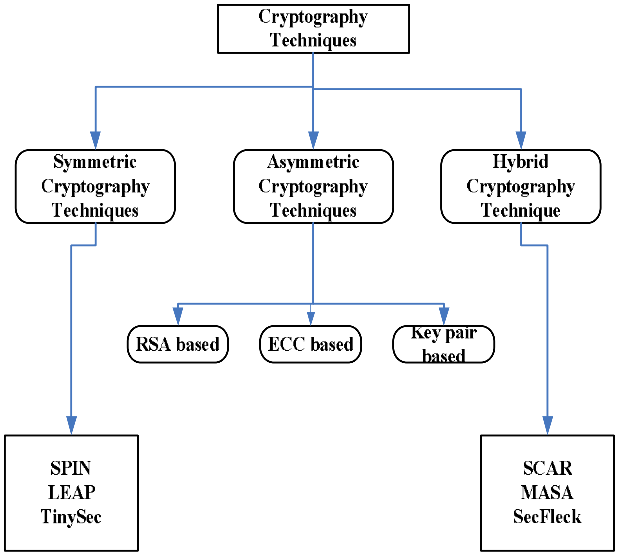
Cryptography Techniques
Symmetric Cryptography Techniques
Asymmetric Cryptography Techniques
Hybrid Cryptography Technique
RSA based
ECC based
Key pair based
SPIN
LEAP
TinySec
SCAR
MASA
SecFleck

Figure 1.Different Cryptography techniques for WSNs

However, WSNs have emerged as a highly active area of research and development for future wireless networks, but it can be seen that the lifetime/lifecycle of a WSN communication route is very much resource constrained. Thus to design an efficient wireless path in sensor communication, selection of a very lightweight cryptography technique is highly desired [6]. This paper aims to introduce a multilayered cryptography based security framework which considers both symmetric and asymmetric cryptosystems for providing considerably more efficient and high level of authenticity on data transferring for conventional WSNs. The experimental outcomes show the effectiveness of the proposed algorithm considering reliable and faster data transmission and further imply comparative analysis on conventional cryptography techniques (Symmetric and asymmetric). The proposed study is organized as follows where section II describes the most significant works which have been carried out till date in the domain of wireless sensor network communication considering secure connection using efficient routing strategies. Section III highlights the overall system design which formulates the design specification of proposed secure routing policy followed by implementation of proposed secure routing protocol PERSI. Section IV discusses the experimental outcomes of the proposed system which also ensure that our proposed scheme outperforms the conventional routing based cryptosystems regarding different performance parameters. Section V highlights the conclusion and summarizes the future work.

II. RELATED WORK

The study of Tan et al [7] introduced an identity based light weight cryptosystem which has been further implemented in wireless body area network. The experimental outcomes of the proposed system show that the proposed system balances both security and privacy in terms of data accessibility, authenticity. The performance analysis of the proposed system shows the effectiveness. In the study of Shuai [8] a sensor data encryption chip core is proposed, which has been conceptualized to enhance safety aspects as well as to improve the multimedia wireless data access through communication channel. The hardware implementation of the proposed protocol shows that it achieves quality processing during the encryption and decryption. The system components are easily configurable with the sensor network. Wei et al [9] proposed an accountable and privacy control mechanism which has been implemented in wireless sensor network communication to ensure better privacy of data and accountability against malicious behaviour of users. A healthcare monitoring architecture has been configured and coupled with wearable sensor systems in the study of Huang et al [10] where the proposed system uses ad hoc mode for a group based data transferring and data access control. The performance analysis of the proposed system shows that it has been verified considering different types of effective performance metrics. Tsai [11] introduced a novel concept of key establishment in wireless sensor networks to overcome various malicious attacks performed by intruders. It also highlights two key re establishment strategy using shared key mechanism. The comparative analysis and the theoretical proof of concepts of the proposed system show the robustness against realistic considerations and real time test bed.

III. System Design and Implementation

This paper aims to design a scalable wireless sensor network protocol namely protocol for exchanging of reliable sensor information (PERSI). The proposed system conceptualized considering secure and efficient routing which enables this protocol as a valid data-centric routing mechanism. The following figure 1 illustrates the design specification associated with the proposed system. It shows that node A will broadcast an advertisement message M_{ad} to its nearest neighbor node B, once it senses some data (several environmental parameters e.g. temperature, humidity, etc.). Therefore, node B will establish radio link connectivity with node A and sends a request M_{Req} message. As per the requesting, node A transmits its respect data packet to node B. After receiving data packets from node A, node B broadcasts advertisement messages to its nearest neighbors and wait for a request to come. All the nodes connected with node B transmit request if they require the particular data. Thus, node B will send and forward its respective data to that particular node on its demand. The proposed protocol uses an efficient hybrid cryptosystem based approach where mutual compromise made for establishing a secure communication in between the sensor nodes.

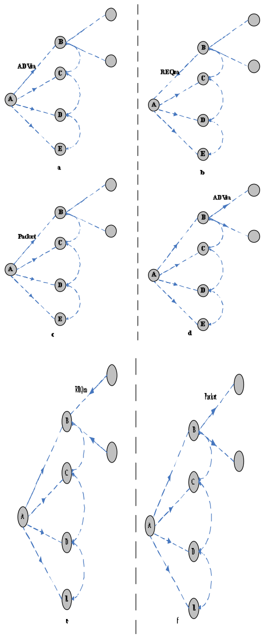

Figure 2.Routing Strategy of the proposed system

The proposed routing model specifically designed to configure into wireless sensor network where the data packet which is forwarded to the next node considered to have two different parts, the initial part is termed as metadata which keeps the record about the actual data where the significant information is stored. The design specification of the data packet format is highlighted below.

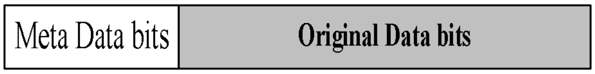

Figure 3.Data packet format in mutual compromise based routing strategy

Therefore, the proposed protocol utilizes the concept of cryptography on both Metadata and the original data. However, the proposed secure algorithm has been designed to implement it in PERSI routing protocol. To implement the proposed fusion based cryptography strategy in PERSI protocol based network model the following design considerations are needed to be followed. The hypothetical assumptions taken to determine salient features associated with the proposed model includes a combined key based very efficient secure routing strategy which further also achieve an effective processing time during long haul execution/simulation period.

Steps to be followed to implement the secure routing strategy for the proposed PERSI protocol
Input: Secret Keys S_k, Hash (f) , Private Key P_k
Output: Installation process of keys in every nodes of the Network
Start

```
1. Initialize → $S_k$
2. Initialize → Hash(f)
3.   for ( i ← 1:n)
4.      Choose ← $node_i$
5.         Assign ← $P_{ki}$
6.      $Dest_{node}$ ← Assign $pub_k$
7.    End for
8. $N_{route}$ ←Store $Pub_{ki}$
9. $N_{route}$← save common $S_k$
```

End

The above process shows the installation of different key components in the entire WSNs model. It also shows how secret keys, private keys are generated and installed in every node of the network using the hash function. The proposed cryptosystem exploits secret keys which are shared among every node where every node also carries a randomly generated private key and its respective public key on the destination node. The process also decomposes the public key component to the all other nodes except its destination node and stores the secret key. The proposed system also introduces a concept where the Meta data is encrypted using a symmetric key based encryption technique along with hash functions. The actual data is encrypted using a public key cryptography and broadcasted into the WSN network. The data encryption using the proposed combined cryptography at the source node, intermediate nodes and the destination node is highlighted using following figure 4.

The below figure 4 shows how the proposed combined key based cryptography technique has been implemented in PERSI protocol. The cryptosystem has been activated in source, intermediate and destination nodes during the initial point of the network lifecycle. In the node of origin, the meta data part of the message will be encrypted using symmetric key composition and hash function where as the actual data will be encrypted using public key structure. The encrypted data will be further broadcasted to the network. The intermediate node will receive the encrypted data packet and will perform data aggregation on the data packet and also symmetric key decomposition after that the data will be compared with the hash function and the aggregated data along with the remaining part will be en route to the destination node. The target node will perform symmetric decomposition using the hash function and also shows public key decomposition to depacketize the original message bits.

IV. RESULT & DISCUSSION

The following figure 5 shows the comparative analysis of the proposed system with respect to the conventional cryptographic schemes which are asymmetric and symmetric cryptographies respectively. The following performance evaluation of the proposed combined key based encryption achieves a reasonable processing time 28 ms where the symmetric cryptosystem achieves very less amount of processing time which 9 ms. But it can be seen that most of the significant studies which have implemented symmetric key cryptography on various routing systems and they have also suggested that it provides very less level of security compared to the asymmetric and our proposed system.

It can also be seen that asymmetric cryptosystems provide better security aspects, but it consumes a very large amount of memory and processing time. The comparative analysis highlights that our proposed cryptography based method works very efficiently in the PERSI protocol and achieves the high level of data security and confidentiality. It also consumes very less amount of resources as compared to the conventional cryptosystems.

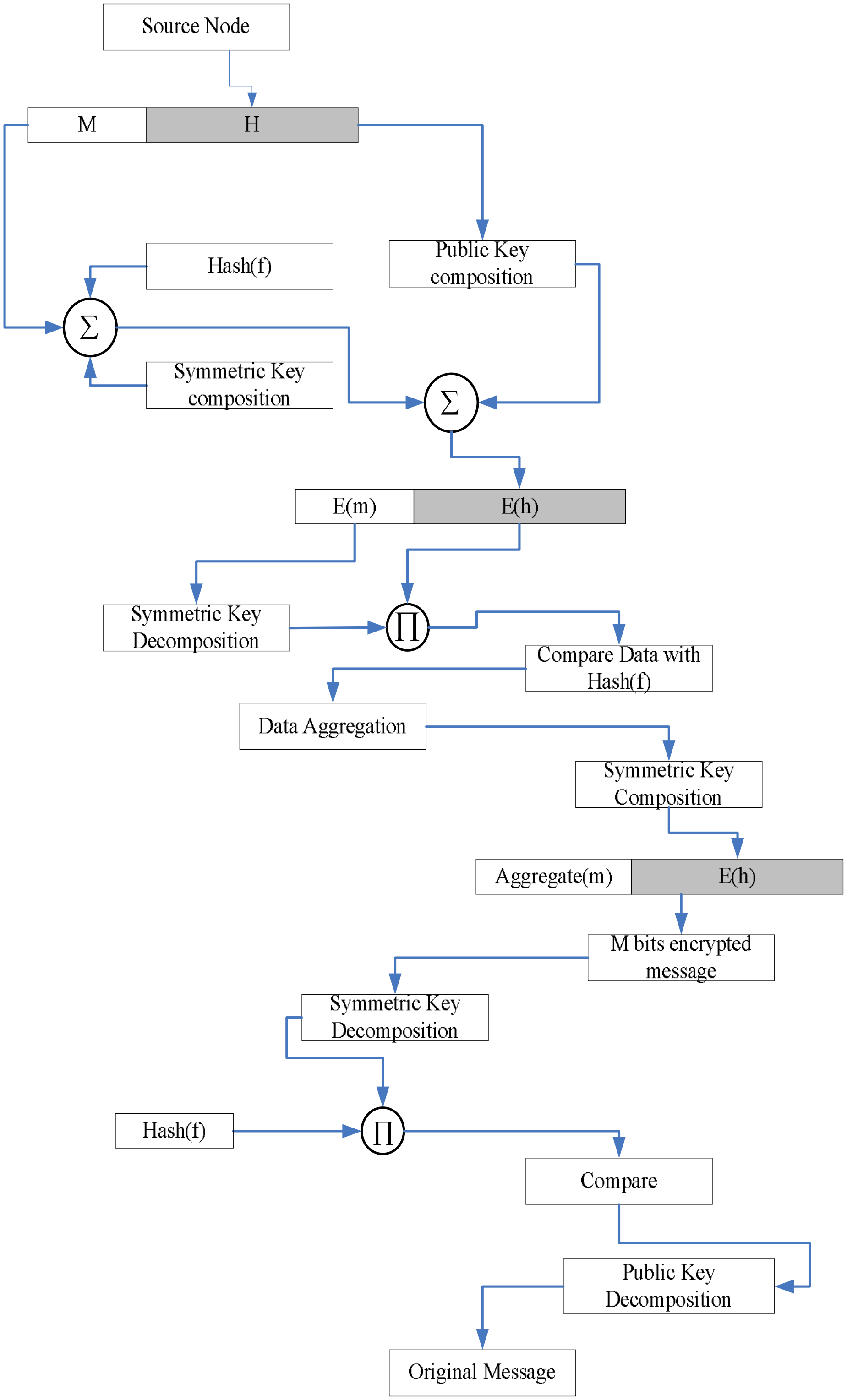

Figure 4.Proposed System Architecture

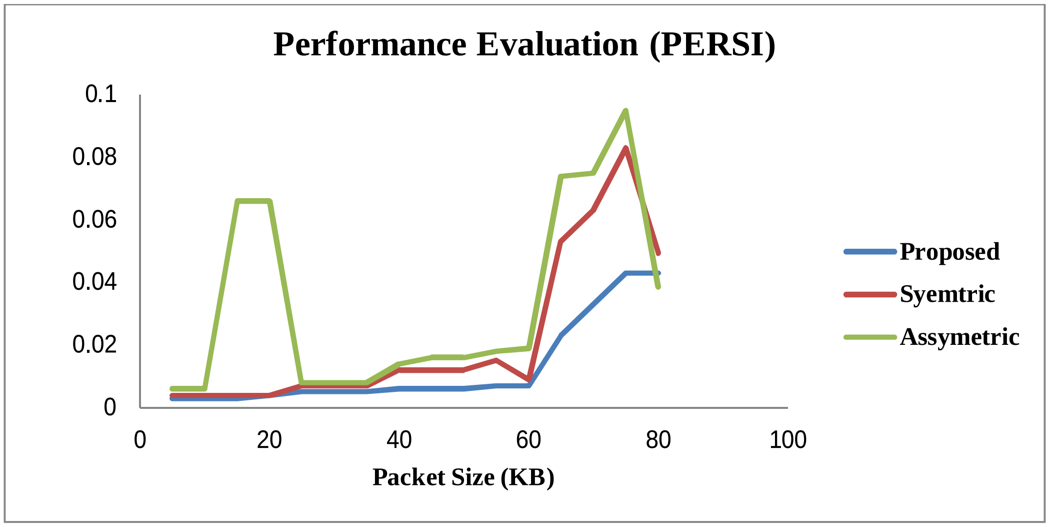

Figure 5.

V. Conclusion

This paper introduces a combined key based analytical model namely, PERSI for exchanging reliable sensor information in wireless sensor networks. The proposed system has been conceptualized considering both symmetric and asymmetric cryptosystem which have been implemented mutually in a real-time test bed. The experimental outcomes of the proposed system show that it achieves the very high level of security along with very less amount of processing speed and resource utilization. The computational complexity of the proposed technique has been found very less as compared to the conventional symmetric, asymmetric cryptography techniques. The proposed system has been coupled with the end to end nodes of a network. It has also been observed in the above stated figure 5 that as long as the packet size increased the processing time also got increased for the proposed cryptosystem. The proposed protocol achieves very high efficiency and faster processing speed and can be configured and integrated easily into future wireless sensor network models.

References

[1] Boukerche, and Ren, Y, "A secure mobile healthcare system using trust-based multicast scheme", Selected Areas in Communications, IEEE Journal, Vol.27(4), pp.387-399,2009

[2] K. Alam, K.R. Alam, O. Faruq, and Y. Morimoto, "A comparison between RSA and ElGamal based untraceable blind signature schemes", In International Conference on Networking Systems and Security (NSysS), pp. 1-4,2016

[3] K. Bicakci, H. Gultekin, and B. Tavli, "The Impact of One-Time Energy Costs on Network Lifetime in Wireless Sensor Networks", IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 12, DECEMBER 2009

[4] R. Dautov, and G.R. Tsouri, "Securing while Sampling in Wireless Body Area Networks with Application to Electrocardiography",IEEE Journal of Biomedical and Health Informatics,2014

[5] F. Delgosha, and F. Fekri, "A multivariate key-establishment scheme for wireless sensor networks", Wireless Communications, IEEE Transactions, Vol.8, No. 4, pp.1814-1824,2009.

[6] L. Harn, C. Hsu, O. Ruan, and M. Zhang, "Novel Design of Secure End-to-End Routing Proto-col in Wireless Sensor Networks", IEEE Sensors Journal Vol. 16, No. 6, 2016

[7] C.C.Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: a lightweight identity-based cryptography for body sensor networks", Information Technology in Biomedicine, IEEE Transactions, Vol.13, No. 6, pp.926-932, 2009

[8] Shuai, and X-Xin, "Research of Cipher Chip Core for Sensor Data Encryption", IEEE Sensors Journal, Vol.16(12), pp.4949-4954,2016

[9] J. Wei, G. Yang, and Y. Mu, "Comments on"Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks"", journal of Latex Class Files, Vol. 14, No. 8, 2015

[10] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks", Selected Areas in Communications, IEEE Journal, Vol.27(4), pp.400-411, 2009.