



DISTRIBUTED POWER CONTROL FOR MULTI-HOP ENERGY HARVESTING LINKS WITH RETRANSMISSION

^[1] Mrs. S,Yoga, ^[2] Mrs. R.Madhumathi, ^[3] C.Kaleeswari, ^[4]S.Pavithra

^[1, 2]Assistant Professor, ^[3, 4] Scholar

^{1, 2, 3, 4} Dept. of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram,
TamilNadu, India.

ABSTRACT:

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this project, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. I have show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

I INTRODUCTION

Wireless Sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption

by using local collaboration among sensor nodes. A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. In this project, for convenience, I have call this sort of cluster-based protocols as LEACH-like proto-cols. Researchers have been widely studying CWSNs in the last decade in the literature. However, the implementation of the cluster-based architecture in the real world is rather complicated. Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs).

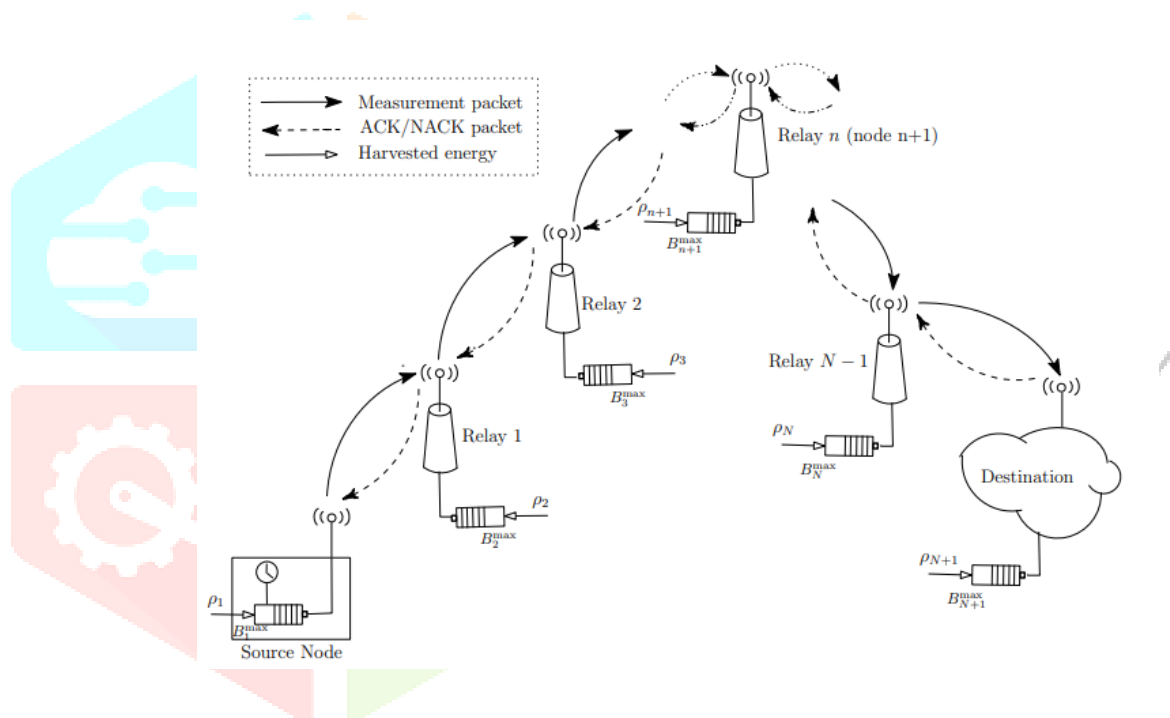


Figure 1: Each node transmits and receives in its assigned sub frame.

To mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pair wise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pair wise keys. Decreases after a long-term operation of the network. Since the more CHs elected by them, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pair wise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate [13]. Wireless sensor network (WSN) is constituted by spatially distributed

autonomous devices communicating wirelessly, gathering information and detecting certain events of significance in the physical and environmental conditions. Each of these devices is capable of concurrently sensing, processing and communicating. Having these capabilities on a sensor device offers a vast number of compelling applications [1]–[5], as illustrated in Fig. 1. For example, one of the oldest application areas of WSNs is found in environmental monitoring, ranging from the tracking herds of animals to the monitoring hard-to-reach areas. Military battlefields also constitute a potential application of WSNs, especially in inaccessible or hostile territory, where WSNs may be indispensable for the detection of snipers, intruders and for tracking their activity.

II LITERATURE SURVEY

[1] JAYDIP SEN, A SURVEY ON WIRELESS SENSOR NETWORK SECURITY:

Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is more critical if the network is deployed for some mission-critical applications such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task.

This project discusses the current state of the art in security mechanisms for WSNs. various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included. In addition to traditional security issues like secure routing and secure data aggregation, security mechanisms deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In real-world WSNs, the nodes cannot be assumed to be trustworthy a priori. Researchers have therefore, focused on building a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms. In this chapter, we present a survey of the security issues in WSNs. First I am outline the constraints of WSNs, security requirements in these networks, and various possible attacks and the corresponding countermeasures. Then a holistic view of the security issues is presented. These issues are classified into six categories: cryptography, key management, secure routing, secure data aggregation, intrusion detection and trust management. The advantages and disadvantages of various security protocols are discussed, compared and evaluated. Some open research issues in each of these areas are also discussed.

Unreliable communication:

Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Furthermore, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission.

[2] S.Ganesh, Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based Dynamic Clustering Mechanisms:

Advances in Wireless Sensor Network Technology (WSN) have provided the availability of small and low-cost sensor with capability of sensing various types of physical and environmental conditions, data processing and wireless communication. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are limited. Triple Umpiring System (TUS) has already been proved its better performance on Wireless Sensor Networks. Clustering technique provides an effective way to prolong the lifetime of WSN.

In this project, we modified the Ad hoc on demand Distance Vector Routing (AODV) by incorporating Signal to Noise Ratio (SNR) based dynamic clustering. The proposed scheme Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based dynamic Clustering mechanisms (ESRPSDC) can partition the nodes into clusters and select the Cluster Head (CH) among the nodes based on the energy and Non Cluster Head (NCH) nodes join with a specific CH based on SNR Values.

III SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. Ancient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

3.2 PROPOSED SYSTEM

In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are ancient in communication and applying the key management for security. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

IV SYSTEM ARCHITECTURE

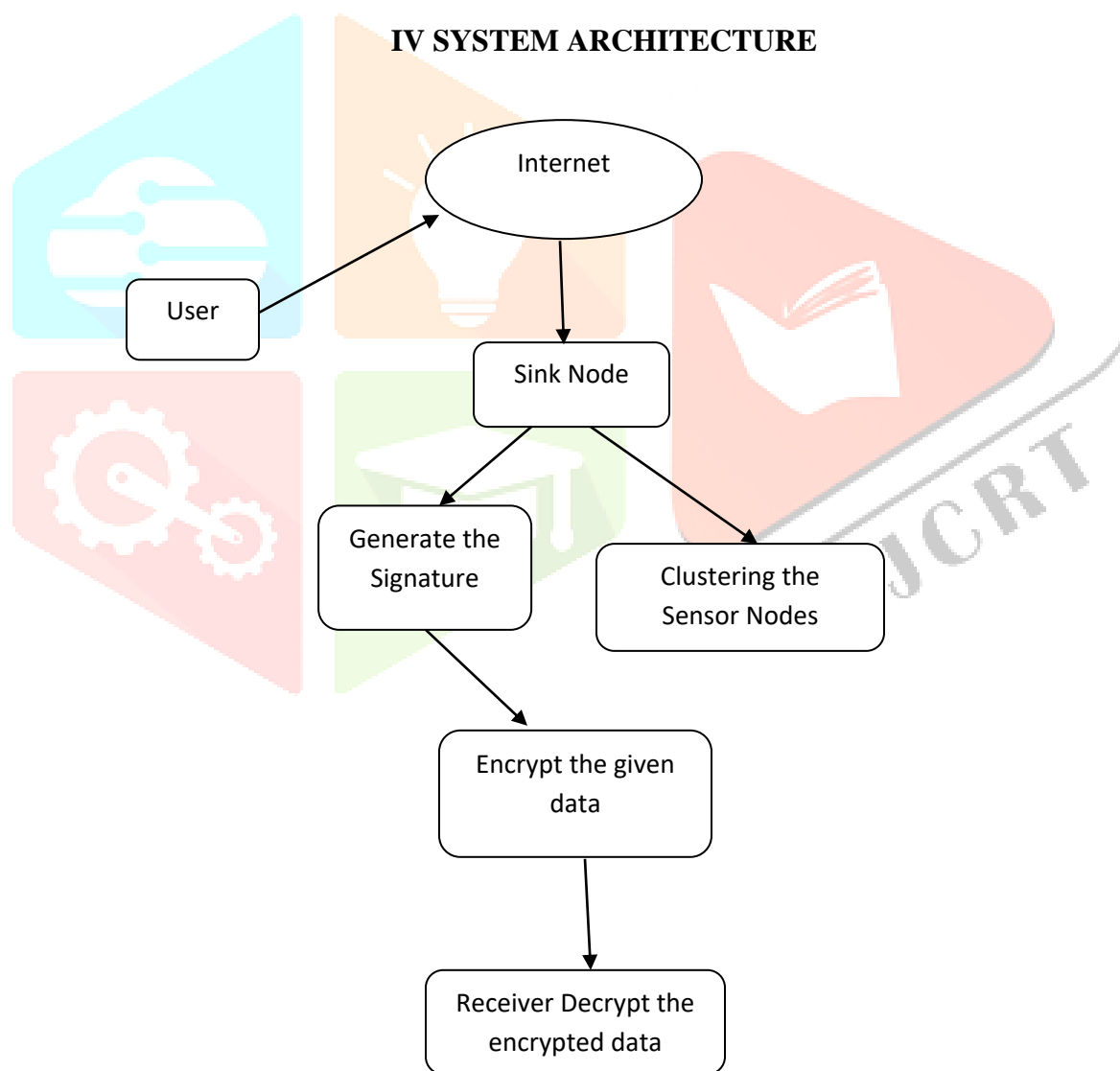


Figure 4.1 Architecture

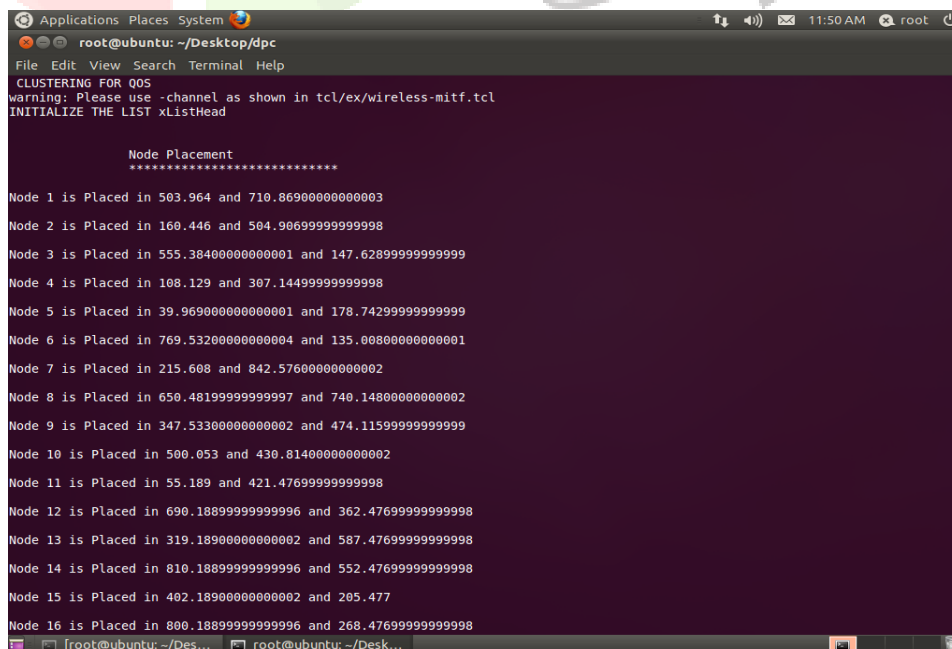
V SYSTEM IMPLEMENTATION

5.1 MODULES

1. SET Protocol
2. Key management for security
 - a. Neighborhood authentication
 - b. Storage cost
 - c. Network scalability
 - d. Communication overhead
 - e. Computational overhead
 - f. Attack resilience

5.2 SET PROTOCOL

In this module, figure 5.1 shows secure and efficient data transmission (SET) protocol for CWSNs. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.



```
Applications Places System
root@ubuntu: ~/Desktop/dpc
File Edit View Search Terminal Help
CLUSTERING FOR QOS
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead

Node Placement
*****

Node 1 is Placed in 503.964 and 710.86900000000003
Node 2 is Placed in 160.446 and 504.906999999999998
Node 3 is Placed in 555.384000000000001 and 147.628999999999999
Node 4 is Placed in 108.129 and 307.144999999999998
Node 5 is Placed in 39.969000000000001 and 178.742999999999999
Node 6 is Placed in 769.532000000000004 and 135.008000000000001
Node 7 is Placed in 215.608 and 842.576000000000002
Node 8 is Placed in 650.481999999999997 and 740.148000000000002
Node 9 is Placed in 347.533000000000002 and 474.115999999999999
Node 10 is Placed in 500.053 and 430.814000000000002
Node 11 is Placed in 55.189 and 421.476999999999998
Node 12 is Placed in 690.188999999999996 and 362.476999999999998
Node 13 is Placed in 319.189000000000002 and 587.476999999999998
Node 14 is Placed in 810.188999999999996 and 552.476999999999998
Node 15 is Placed in 402.189000000000002 and 205.477
Node 16 is Placed in 800.188999999999996 and 268.476999999999998
```

Figure 5.1 Node Placement

5.3 KEY MANAGEMENT FOR SECURITY

In this module, security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications.

5.3.1 KEY MANAGEMENT

In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

A. NEIGHBORHOOD AUTHENTICATION

In this module, figure 5.2 used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, “limited” means the probability of neighborhood authentication, where only the nodes with the shared pair wise key can authenticate each other.

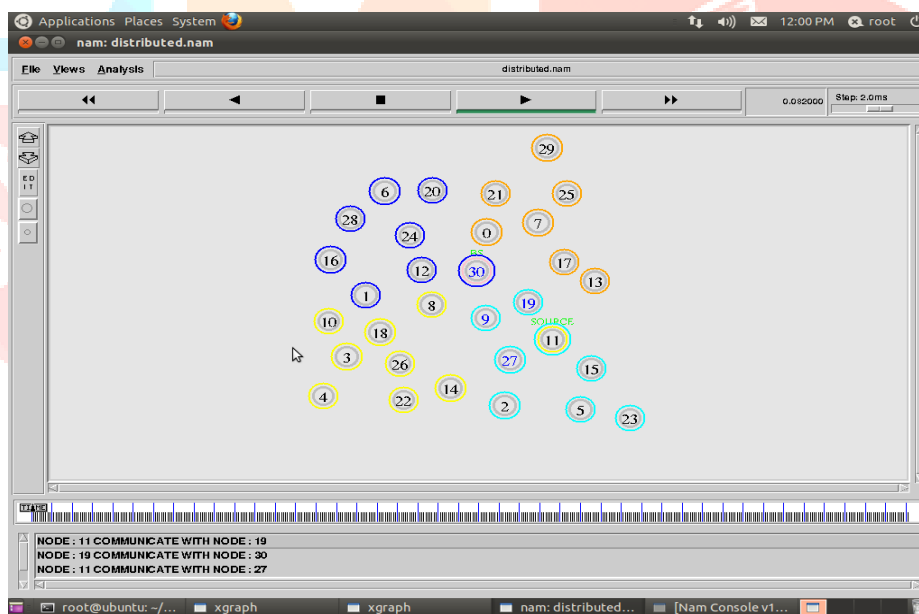


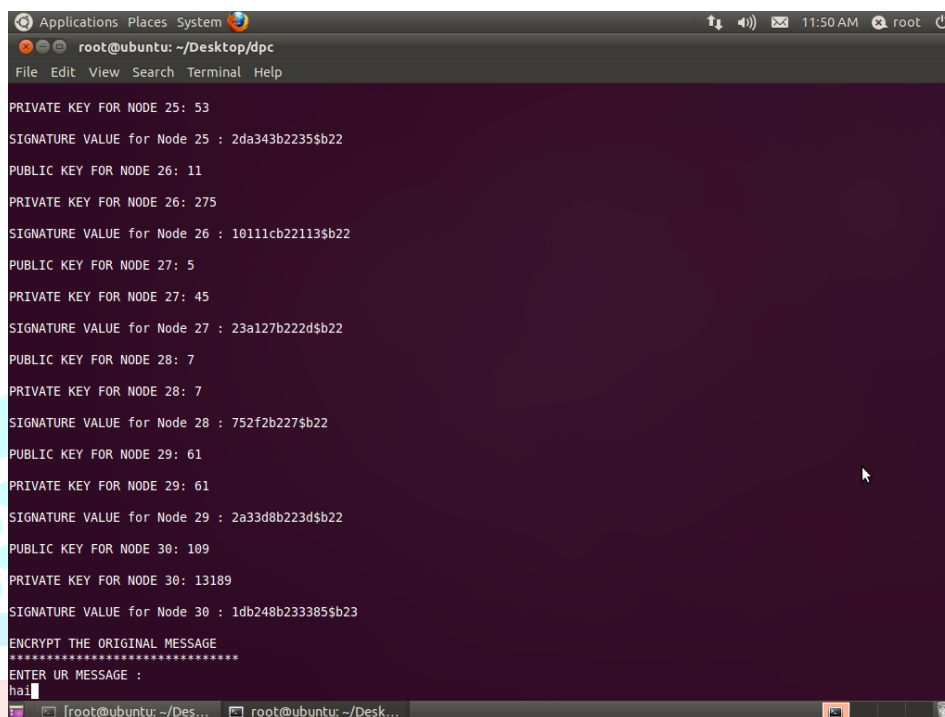
Figure 5.2 Neighborhood authentication

B. STORAGE COST

In this module, represents the requirement of the security keys stored in sensor node’s memory.

C. NETWORK SCALABILITY

In this module, figure 5.3 indicates whether a security protocol is able to scale without compromising the security requirements. Here, “comparative low” means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network.

A terminal window on an Ubuntu system showing the output of a key generation script. The terminal title is 'root@ubuntu: ~/Desktop/dpc'. The output lists private and public keys and signature values for nodes 25 through 30. At the bottom, it prompts for a message to encrypt, with 'hai' entered.

```
PRIVATE KEY FOR NODE 25: 53
SIGNATURE VALUE for Node 25 : 2da343b22355b22
PUBLIC KEY FOR NODE 26: 11
PRIVATE KEY FOR NODE 26: 275
SIGNATURE VALUE for Node 26 : 10111cb221135b22
PUBLIC KEY FOR NODE 27: 5
PRIVATE KEY FOR NODE 27: 45
SIGNATURE VALUE for Node 27 : 23a127b222d5b22
PUBLIC KEY FOR NODE 28: 7
PRIVATE KEY FOR NODE 28: 7
SIGNATURE VALUE for Node 28 : 752f2b2275b22
PUBLIC KEY FOR NODE 29: 61
PRIVATE KEY FOR NODE 29: 61
SIGNATURE VALUE for Node 29 : 2a33d8b223d5b22
PUBLIC KEY FOR NODE 30: 109
PRIVATE KEY FOR NODE 30: 13189
SIGNATURE VALUE for Node 30 : 1db248b233385b23
ENCRYPT THE ORIGINAL MESSAGE
*****
ENTER UR MESSAGE :
hai
```

Figure 5.3 Key Generation

D. COMMUNICATION OVERHEAD

In this module, the security overhead in the data packets during communication.

E. COMPUTATIONAL OVERHEAD

In this module, the energy cost and computation efficiency on the generation and verifications of the certificates or signatures for security.

F. ATTACK RESILIENCE

In this module, the types of attacks that security protocol can protect against.

VI CONCLUSION

I am first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. Then I have presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, I have provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. And RSA algorithm have Asymmetric Key for protect our data during transmission. RSA is used for sender encrypt the data and receiver decrypt the data. Lastly, the comparison in the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, I am pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

VII FUTURE ENHANCEMENT

Future extensions of this work can consider the design of RIPs for multi-hop links with time-correlated channels, and under different quality of service requirements. First, I am considered a scenario when the energy cost for reception is negligible, and derived closed-form expressions for the optimal RIPs. Next, I have presented an iterative geometric programming based solution to the RIP optimization problem under non negligible energy reception cost. Through simulations, I illustrated that our proposed policies significantly outperform equal power policies and achieve a performance close to the lower bound. In addition, our results provided interesting insights into the trade-offs in the system parameters and highlighted the coupled nature of the problem.

REFERENCES

1. T. Hara, V.I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
2. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Comm. Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
3. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
4. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," *IEEE Trans. Wireless Comm.*, vol. 1, no. 4, pp. 660-670, Oct. 2002.
5. A.Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel & Distributed Systems*, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
6. S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 14/15, pp. 2842-2852, 2007.
7. K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int'l J. Computer Applications*, vol. 47, no. 11, pp. 23-28, 2012.

8. L.B. Oliveira et al., "Sec LEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
9. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
10. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
11. S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
12. G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.
13. W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
14. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
15. D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.
16. R. Yasmin, E. Ritter, and G. Wang, "An Authentication Frame-work for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

