Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication and Key Distribution Schemes for Wireless Sensors Network

Shweta Goel , Manjeet Behniwal, Ajay Kumar Sharma
Computer Science&KUK University
Kurukshetra, India

Abstract- Wireless sensor network contains sensor nodes having limited capabilities to sense, collect, and manipulate the data. The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multi-hop may weaken the security strength. There may be different types of attack which can modify the sensed data by capturing the intermediate nods. Therefore, security services, such as, authentication and key establishment between sensor nodes, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. In this paper we proposed a mutual authentication method based on public key distribution technique, which can be used to secure the sensor network and we will also analyze the impact of this method over the network performance.

Keywords- Wireless sensor networks, WSN, Security, Attacks, key distribution, cryptography

I. INTRODUCTION

Wireless sensor network is one of remarkable technologies for ubiquitous computing environment to enable an end-user to gather the nearby context information. Typical examples of this network are location supporting application for indoor environment and environment monitoring application. In these applications, user mobility should be considered in authentication process. However, the existing approaches do not considered this issue. Node should perform authentication procedure again after the node moves another position. [11][12]

A. Security challenges in wireless sensor networks

Security challenges in WSN are as follows:

- Minimizing resource consumption and maximizing security performance.
- Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
- In-network processing involves intermediate nodes in end-to-end information transfer.
- Wireless communication characteristics render traditional wired-based security schemes unsuitable.
- Large scale and node mobility make the affair more complex.
- Node adding and failure make the network topology dynamic.[12]

B. Attacks on wireless sensor network

i) Active Attack

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.[11][12]

ii) Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. [11][12]

C. Cryptography techniques and key distribution methods

Cryptography is a technique to secure the data. It uses the concept of keys to change the form of input data, called encryption and data can be converted to previous form using the same keys, called decryption. [11]

D. Types of Cryptography

- Public Key Cryptography: In this method, two different keys are used to secure the data. Public key is available to everyone and private key is kept secret. Sender can send the data to receiver by encrypting the data using his public key and receiver can decrypt the data using the its private key. [11]
- Private Key Cryptography: In this method, a group of user share same key. Sender can send the encrypted data using private key and receiver can decrypt the data using same key. [12]

E. Key distribution methods

- Pre-distribution of keys: In this method, keys are assigned to each node for secure communication. Nodes can use these keys to share the data over network in a secure manner.
- Post-distribution of keys: in this method, keys are assigned after the node deployment. Nod can obtained the keys from base station.[12]

F. Selection of Key distribution method

Selection of cryptography method is a very critical issue for security implementation in WSNs. Many researchers consider that asymmetric key cryptography methods are not suitable for WSNs due to the resource limitation of sensor nodes. Although some recent research results show that it is feasible to apply asymmetric key cryptography to WSNs by choosing appropriate algorithms, parameters, etc., Key management is still too expensive in terms of computation and energy cost for sensor nodes, and still need further research. Symmetric key cryptography is more efficient then public key cryptography in terms of speed and low energy cost. However, the key management is not an easy task for symmetric key cryptography. There is need to develop more efficient and flexible key management scheme for WSN. [11]

II. LITERATURE REVIEW

Wireless sensor network is insecure by its nature: there is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the network. As a result, compared with the wired network, the wireless network will need more robust security scheme to ensure the security of it. [1][12]

Researchers have developed lot of different methods to secure the sensor network but each method has some sort of limitations. Three are some critical operations like node authentication and key distribution. Now we will discuss the different schemes of authentication and key distribution used by the researchers.

J. Kim, J. Baek, T. Shon [1] suggested an efficient method of membership verification for re-authentication of mobile node and shows the performance analysis of our membership verification. Using this method, they proposed an efficient and scalable re-authentication protocol over wireless sensor network. Also, they provided performance and security analysis of the protocol.

H. Wang and Y. Zhang [2] proposed an efficient threshold self-healing key distribution scheme with sponsorization for infrastructure less wireless networks. They claimed that the key distribution scheme satisfies the forward security, i.e., any internal user who has been revoked cannot generate a new session key. In this paper, an attack method against this key distribution scheme's forward security was presented. Furthermore, this attack method can also be applied to this scheme's backward security. Thus, the original threshold self-healing key distribution scheme is insecure.

K. Han, T. Shon and K. Kim [3] extend our novel and efficient node authentication and key exchange protocol that support Irregular distribution. Compared with previous protocols, this protocol has only a third of communication and computational overhead. The proposed improvement enables the efficient node re-authentication and key exchange even when the sensors are irregularly distributed to the smart home and WPAN for supporting various convergence services. In order to verify the proposed approach, they performed three kinds of validation according to communication pass, message size, and security analysis. From the analysis, improvement guarantees the longer lifetime of Smart Home Devices and WPAN while providing security solutions. In future work they will deploy the proposed approach to real Smart home environments and confirm the authentication operations for supporting NSL.

W. Wang and D. Peng [4] proposed a quality-driven scheme to optimize stream authentication and unequal error protection (UEP) jointly. This scheme can provide digital image authentication, image transmission quality optimization, and high energy efficiency for WMSN. The contribution of this research is two-fold as summarized below. First, a new resource allocation aware greedy stream authentication approach is proposed to simplify the authentication process. Second, an authentication-aware wireless network resource allocation scheme is developed to reduce image distortion and energy

consumption in transmission. The scheme is studied by unequally protected image packets with the consideration of coding and authentication dependency.

The proposed a methodology for quality-driven and energy-efficient transmission of authenticated images in WMSNs. First, a JPEG2000 compatible stream authentication scheme is proposed with a minimal authentication dependency overhead, which is very easy to be integrated with network resource allocation schemes in order to tackle the problem of severe energy constraints in WMSNs. Furthermore, a general UEP-based network resource allocation framework is developed to optimize the image transmission quality with integrity and energy efficiency assurance. Simulation results demonstrated that the proposed schemes significantly improved the authenticated image quality even under strict communication energy consumption constraints in wireless multimedia sensor networks.

A. Rasheed and R. N. Mahapatra [5] proposed a general three-tier security framework for authentication and pair-wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Analysis indicates that with 10 percent of the sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach. They have further improved the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes. They used the one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.

H. Dai and H. Xu [6] a new key pre-distribution algorithm based on matrix-based technique was proposed and numerically evaluated. The proposed approach combines matrix-based method and polynomial-based key pre-distribution approach to achieve both high network connectivity and strong resilience against node capture. The effectiveness of the proposed algorithm has been demonstrated through analysis and simulation. Also, an efficient encoding mechanism was designed to optimize the memory overhead. In our future work, they plan to develop the group-based matrix decomposition for the large distributed WSNs.

T. Kwon and J. Hong [7] proposed X-TESLA, an efficient scheme which may continue indefinitely and securely, that addresses this and many other issues of the previous schemes. With the advent of more powerful sensor node commodities such as iMote2, the future of public-key technique application to broadcast authentication looks bright, but X-TESLA can efficiently be combined with public-key techniques also. For example, they could modify X-TESLA to use digital signatures on Type 4 packets, keeping everything else the same. Through the application of TMD-tradeoff techniques they observed that care should be taken with the short-key-chain based broadcast authentication schemes.

Z. Liu, J. Ma Q. Huang, and Sang Jae Moon [8] presented an Asymmetric Key Pre-distribution Scheme. Instead of assuming that the network is comprised entirely of identical users in conventional key pre-distribution schemes, the network now consists of a mix of users with different missions, i.e., ordinary users and keying material servers. A group of users, using secret keys preloaded in their memory and public keying material retrieved from one keying material server, can compute a session key. The properties of this method are that, the compromise of keying material servers does not reveal any information about users' secret keys and the session keys of privileged subset of users; if computational assumptions are considered, each user has very low storage requirement. These properties make it attractive for sensor networks. They first formally define the asymmetric key pre-distribution scheme in terms of the entropy and give lower bounds on user's storage requirement and the public keying material size. Then, they presented its constructions and applications for sensor networks.

P. F. Oliveira and J. Barros [9] considered the problem of secret key distribution in a sensor network with multiple scattered sensor nodes and a mobile device that can be used to bootstrap the network. Their main contribution is a set of secure protocols that rely on simple network coding operations to provide a robust and low-complexity solution for sharing secret keys among sensor nodes, including pairwise keys, cluster keys, key revocation, and mobile node authentication. Despite its role as a key enabler for this approach, the mobile node only has access to an encrypted version of the keys, providing information- theoretic security with respect to attacks focused on the mobile node. Results include performance evaluation in terms of security metrics and a detailed analysis of resource utilization. The basic scheme was implemented and tested in a real-life sensor network test bed. This class of network coding protocols to be particularly well suited for highly constrained dynamic systems such as wireless sensor networks.

K. Lu, Yi Qian, M. Guizani, and H. H. Chen [10] proposed a unified framework for distributed key management schemes in heterogeneous wireless sensor networks. Analytical models are developed to evaluate its performance in terms of connectivity, reliability, and resilience. Extensive simulation results show that, even with a small number of heterogeneous nodes, the performance of a wireless sensor network can be improved substantially. It is also shown that our analytical models can be used to accurately predict the performance of wireless sensor networks under varying conditions.

Problem Formulation

WIRELESS sensor networks are dense wireless networks of sensor nodes collecting and disseminating environmental data. Sensor nodes are small low-power devices constrained severely in their computation, communication, and storage capabilities, usually for economical reasons. They may sense around themselves, communicate over wireless

channels within short ranges, and frequently fall into the sleep mode for saving their power. Accordingly, a large scale wireless sensor network is composed of a number of sensor nodes for covering wider area through multi-hop connections. It has various kinds of promising applications that include environmental monitoring. Since sensor nodes are deployed in unattended fashions or even in hostile environments, they can readily be captured and tampered by adversaries as well as communication links are compromised. [7]

To secure the communication over WSN there must be a authentication method which can ensure that unauthorized sensors cannot join the network as well as they cannot transmit the data over network.

III. AUTHENTICATION ISSUES FOR WSN

A. Authentication of Sensors

Sensor node can join the network at any time and can start communication over network but unauthorized node can join the network to access the data. So authentication of the nodes is essential. If nodes change their position dynamically then node re- authentication is required.

B. Authentication of data

Sensors communicate with each other by sending the messages to each other. Each sensor should be able to verify the signature of the received message as well as the source of the message because attacker can also transmit the same messages.

C. Authentication of Key pair

It is very difficult to ensure that the keys which are being used in communication are the genuine keys. Intruder can also generate a key pair in order to replace the original one. After the replacement of keys, nodes may use the fake keys and the entire network can be compromised.

We used NS-2 for implementation using two different simulation scenarios and analyzed the performance of the network. The following algorithm can be used to provide the security for the communication over WSN.

IV. PROPOSED METHODOLOGY

We used NS-2 for implementation using two different simulation scenarios and analyzed the performance of the network. The following algorithm can be used to provide the security for the communication over WSN.

List of Abbreviations:

WSN_n	Wireless Sensor Network
S_n	Sensor node
N	Number of Sensor Nodes
P	Global Key Pool for all Sensor Nodes and KDC
K_i	Key Pool for Sensor Node
E	Encryption Algorithm
D	Decryption Algorithm
M	Message
C	Cipher Text
N_{Id}	Node ID
KDC	Key Distribution Center (offline)
U_i	Public Key
PT	Plan Text

A. Key Generation and initialization

For key generation in RSA, we require prime numbers, on the basis of these all keys are generated during secure communication. Before the deployment of sensor nodes, KDC generates public key U_i for each sensor node which is stored in the global key pool P and key pool of sensor node K_i. G_i key can be used as a common key for a particular group of sensor nodes. After key distribution KDC will become offline.

1. U_i generated by KDC : $U_i = Pi \parallel Q_n$

2. $S_n \rightarrow K_i = U_i$
3. $P \rightarrow K_i = U_i$

B. Neighbor selection and Data transfer

After this private and public keys are distributed, Sender encrypts the data with its public key and sends it to the receiver. Receiver receives the message and decrypt it with private key and it also checks the hash code of the message before accepting it. Without using the keys nodes cannot transmit the data. When sender S has some data to send to its neighbor, it initiates the process of mutual authentication. Receiver receives the message and calculates E mod N. If this is a valid public key, only then data transfer starts. After every data transfer, keys are updated so this scheme prevents from various types of attacks which we discussed earlier. Every node follows the steps given below:

get_initial_Data(Prime Numbers p,q) from KDC and calculate n=calculate_product(p,q)

E=Calculated_Keys (n, M_n)

S_n ->Dn= Generated_Keys(n, M_n)

Before data transfer sender repeat the following steps:

authentic =Mutual_AuthenticationProcess(Sender, Receiver)

if (authentic)

{

$C = M^E \bmod n$

Send_Data(C, Receiver)

}

Else

{

Send_Data(false)

}

C. Receiver repeat the following steps

Receiver receives the data extract the plan text and it calculates the Hash value of the received data. If Hash value of plan text is equal to the sent data, only then it accepts the text otherwise it will reject it.

$PT = C^D \bmod n$

HashCodeResult =HashCalculated(PT)

If (HashCodeResult)

{

accept_Data(PT)

}

Else

{

accept_Data(false)

}

D. Secure Data Communication and mutual Authentication Process

Sensors can also update the key pairs as per following steps: Before key update, first of all the previous keys are calculated, if they are same that means nodes in communication are authentic and can update the keys and finally from key pool, new keys are assigned. These steps are repeated again after each successful communication.

If (old_key($S_{ni} \rightarrow E_i == S_{nn} \rightarrow E_j$))

{

Calculate n=p*q

Check_e_=Calculate $S_{ni} \rightarrow E_i \bmod n$

Check_d_=Calculate $S_{nn} \rightarrow D_j \bmod n$

If (Check_e_== S_{nn} -> E_j)
{
authentic=true
}
else
{
authentic=false
}
If (authentic)
{
keyUpdate(S_{ni} ->keypair, S_{nn} -> keypair)
}
}

We used NS-2 for the implementation of proposed scheme using RSA. We used different simulation scenarios using different set of nodes i.e. 10, 20, 30 nodes etc.

V. RESULTS AND DISCUSSION

A. *Communication in normal condition and secure condition-Node:10, 20, 30 nodes*

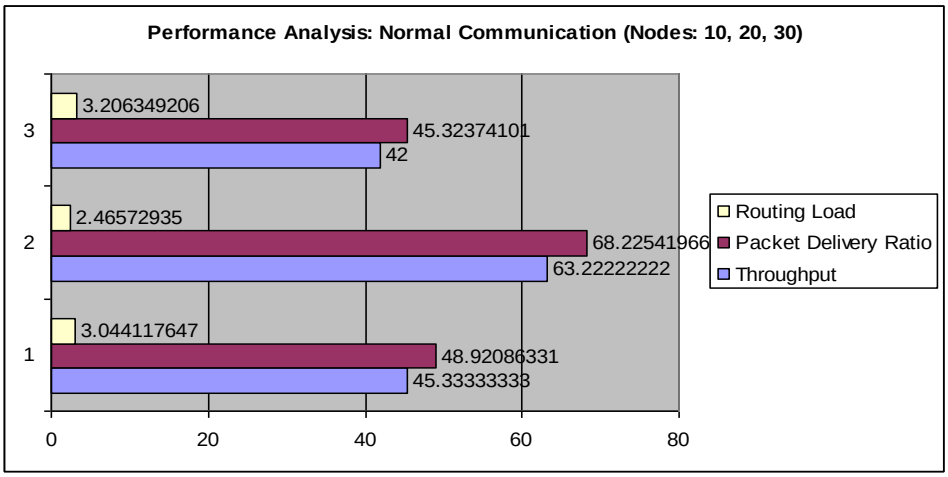

Fig. 1 Performance analysis (in normal condition)

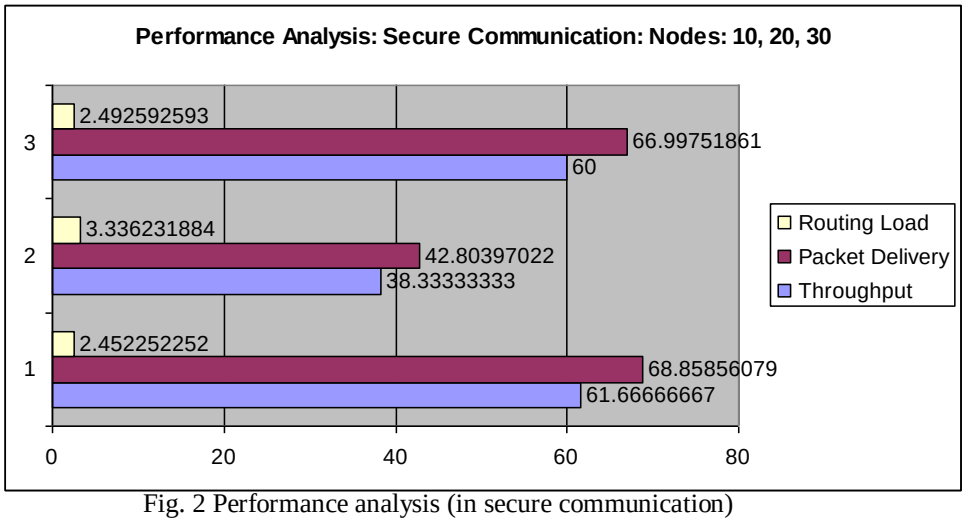

Fig. 2 Performance analysis (in secure communication)

Energy consumption

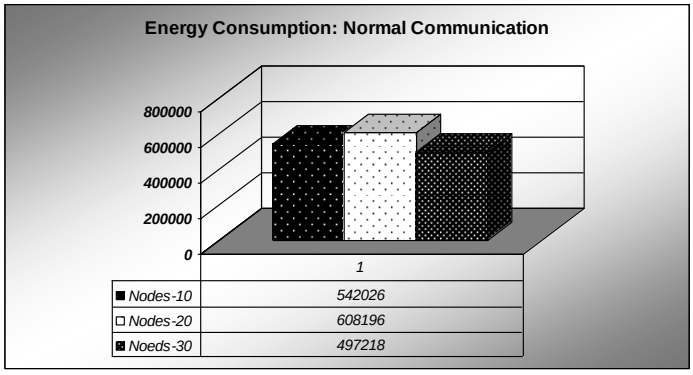

Fig. 3 Energy Consumption (normal communication)

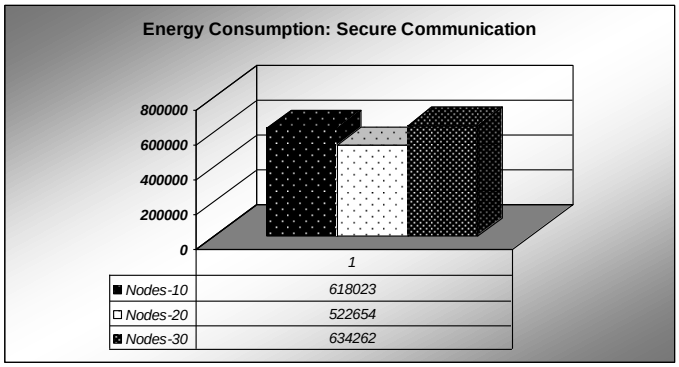

Fig. 4 Energy consumption (Secure Communication)

We can analyze that there is variation in energy consumption. In case of 20 nodes, it has maximum value because of large amount of packet transmission as compared to others.

B. Performance Analysis Table

TABLE I

PERFORMANCE ANALYSIS: COMMUNICATION IN NORMAL CONDITION

Parameters	**Nodes 10**	**Nodes 20**	**Nodes 30**
Packets Sent	834	834	834
Packet Received	408	569	378
Throughput	45.33333333	63.22222222	42
PDR	48.92	68.22	45.32
Routing Load	3.044117647	2.46572935	3.206349206
Energy Consumption	542026	608196	497218

TABLE II

PERFORMANCE ANALYSIS: COMMUNICATION WITH SECURE METHOD

Parameters	**Nodes 10**	**Nodes 20**	**Nodes 30**
Packets Sent	806	806	806
Packet Received	555	345	540
Throughput	61.66666667	38.33333333	60
PDR	66.37	42.80	66.99
Routing Load	2.452252252	3.336231884	2.492592593
Energy Consumption	618023	522654	634262

VI. CONCLUSION

In this paper, we implemented a mutual authentication method based on the public key cryptography. After using this scheme, we measured the performance of entire network using different parameters like Throughput, Load, PDR and energy consumption etc. For message authentication, during communication, encrypted message is sent by the nodes over network, and its HASH is calculated, by sender and receiver decrypts the message and calculates the HASH again. If both HASH values are same, only then, it receives the message otherwise it just rejects it.

For nodes authentication, Every time, a new key is calculated and shared by the neighbors and the operation explained above is repeated. We divided our scenario in to two categories, one is normal communication and other is secure communication. On the basis of average calculation which is based upon the performance of entire network in each scenario, we can analyze that during normal communication, network has the highest Throughput as compared to the Throughput of secure communication. In case of Packet delivery ratio and Routing Load, there are some variations. Secure communication consumes slightly more energy as compared to the normal communication. But in order to secure the network, we can afford this amount of energy consumption.

Finally we can conclude that proposed scheme is capable to provide the confidentiality and integrity but it has an little bit impact on the network performance but in order to achieve the security goals, we can compromise with the performance of network because these days, network security is very essential as compared to the resource consumption.

REFERENCE

[1] Jangseong Kim, Joonsang Baek, Non-member, IEEE, Taeshik Shon, Member, IEEE," An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network", IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011

[2] Huaqun Wang and Yuqing Zhang, " Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 1, JANUARY 2011

[3] Kyusuk Han, Taeshik Shon, Member, IEEE, and Kwangjo Kim, Member, IEEE," Efficient Mobile Sensor Authentication In Smart Home and WPAN", IEEE-2010

[4] Wei Wang, Member, IEEE, Dongming Peng, Member, IEEE, Honggang Wang, Member, IEEE, Hamid Sharif, Senior Member, IEEE, and Hsiao-Hwa Chen, Fellow, IEEE, "A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks With Stream Authentication", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 5, AUGUST 2010

[5] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks', IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012

[6] Hangyang Dai and Hongbing Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE SENSORS JOURNAL, VOL. 10, NO. 8, AUGUST 2010

[7] Taekyoung Kwon, Member, IEEE, and Jin Hong," Secure and Efficient Broadcast Authentication in Wireless Sensor Networks", IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 8, AUGUST 2010

[8] Zhihong Liu, Jianfeng Ma, Member, IEEE, Qiping Huang, and SangJae Moon, Member, IEEE," Asymmetric Key Pre-Distribution Scheme for Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009

[9] Paulo F. Oliveira, Student Member, IEEE, and João Barros, Member, IEEE," A Network Coding Approach to Secret Key Distribution", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 3, SEPTEMBER 2008

[10] 10 Kejie Lu, Yi Qian, Mohsen Guizani, and Hsiao-Hwa Chen," A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 2, FEBRUARY 2008

[11] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009

[12] C Siva Ram Murthy,"Wireless Ad hoc Network-Architectures and Protocols",Pearson-2012

