IJRRECS/October 2015/Volume-3/Issue-10/4677-4681 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SCALABLE MECHANISM FOR DATA TRANSMISSION IN WIRELESS SYSTEMS

S.Himabindu[1], S.Radha[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy College of Engineering, Hyderabad, TS, India

[2]Assistant Professor, Dept of CSE, Malla Reddy College of Engineering, Hyderabad, TS, India

ABSTRACT:

Wireless system networks were emerged as the major electrifying areas in the research of Computer Science over several years. Wireless Sensor Networks make use of minute, reasonably priced sensor nodes by means of a number of unique features. Clustering is a novel and effective means for improving of system performance of sensor networks. In the recent days, the approach of Identity-basis digital signature was developed as key management for security in sensor networks. We study data transmission approach which is novel and effective for cluster-based networks in which clusters are produced dynamically. To reduce storage expenses of signature processing, the online or offline digital signature scheme that is Identity-based was proposed. Our work will recommend data transmission approaches known as Identity-basis digital signature and online or offline digital signature scheme that is Identity-based were proposed for cluster based sensor networks. The proposed approaches validate the encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication and apply the key management in support of security.

Keywords: Wireless system, Clustering, Identity-basis digital signature, Key management, Packets, Cluster-based networks.

1. INTRODUCTION:

A Wireless system network will include huge number of sensors, which are small devices that are capable of sensing physical environment, processing of data and communicate wirelessly to other sensors. Each of the sensors within a sensor network contains assured constraints regarding its source of energy, power and computational abilities. Wireless Sensor Networks have extremely short processing power as well as radio ranges and authorize extremely small energy expenditure and carry out restricted as well as definite monitoring functions [1]. Secure transmission of data is demanded in most of the realistic sensor networks. Clustering is an effective means for recovering the system performance of sensor networks and the data transmission based on clusters were examined by researchers for attaining of network management that improves node lifetime as well as decrease bandwidth consumption by means of usage of local collaboration between sensor nodes. Our work will study data transmission approach which is novel and effective for cluster-based networks in which clusters are produced dynamically [2][3]. We propose two data transmission approaches known as Identity-basis digital signature and online or offline digital signature scheme that is Identity-based were proposed for cluster based sensor networks. In these protocols, secret keys along with pairing parameters are distributed in the entire sensor nodes by means of base station initially, that overcomes the problem of key escrow. These protocols will resolve orphan node difficulty in data transmission by means of a symmetric key management. Digital signature is most crucial services of security that is offered by cryptography in asymmetric systems of key management, in which binding among public key as well as recognition of signer is obtained by means of digital certificate.

2. METHODOLOGY:

In the cluster-basis sensor network system, each of cluster contains leader sensor node, that represent cluster head which makes collection of data that is saved by leaf nodes in cluster, and forward aggregation towards base station. In the network system of cluster basis networks consists of an unchanging base station and huge number of wireless nodes that are uniform in capabilities. The approach of identity-basis digital signature is on the basis of complexity of factoring of integers from

identity-basis cryptography, which develop an entity public key from the identity information. The online or offline digital signature scheme that is Identity-based was proposed to decrease storage expenses of signature processing. This scheme might be effectual for key management in wireless systems and particularly offline phase is implemented on sensor node while the online phase is implemented throughout communication. Our work will propose two data transmission approaches known as Identity-basis digital signature and online or offline digital signature scheme that is Identity-based were proposed for cluster based sensor networks. Basic view of the proposed approaches of Identity-basis digital signature and online or offline digital signature scheme that is Identity-based is to validate the encrypted sensed information, by means of application of digital signatures towards message packets, that are competent in communication and apply the key management in support of security. Online or offline digital signature scheme that is Identity-based is projected to diminish computational cost for security, in which security depends on stability of discrete logarithmic difficulty [4]. Identity-basis digital signature and online or offline digital signature scheme that is Identity-based will resolve orphan node difficulty in data transmission by means of a symmetric key management. Protected communication in identity-basis digital signature depends on identity based cryptography, where user public keys are their identity information and hence users will get hold of equivalent private keys devoid of secondary data transmission, that is competent in communication and save up energy. In projected protocols, secret keys along with pairing parameters are distributed in the entire sensor nodes by means of base station initially, that overcomes the problem of key escrow [5].

3. AN OVERVIEW OF PROPOSED SYSTEM:

The possibility of asymmetric key management was made known in wireless systems in recent times that recompense deficiency from application of symmetric key management that is intended for security. Our work studies data transmission approach which is novel and effective for cluster-based networks in which clusters are produced with dynamism. Data transmission on basis of clusters was examined by researchers for attaining of network

management that improves node lifetime as well as decrease bandwidth consumption. In cluster-basis networks, each cluster contains leader sensor node that represent cluster head which makes collection of data that is saved by leaf nodes in cluster and convey aggregation towards base station. Identity-basis digital signature as well as online or offline digital signature scheme that is Identity-based were proposed for cluster based sensor networks. Identity-basis digital signature is on the basis of complexity of factoring of integers from identity-basis cryptography. The online or offline digital signature system that is Identity-based was proposed to decrease storage expenses of signature processing. It is proposed to diminish computational cost for security, in which security depends on stability of discrete logarithmic difficulty. Proposed approaches authorize the encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication. These schemes will resolve orphan node difficulty in data transmission by means of a symmetric key management. In the network system of cluster basis networks consists of an unchanging base station and huge number of wireless nodes that are uniform in capabilities. Base station is always consistent specifically it is a trustworthy authority. For the meantime, sensor nodes might be compromised by means of attackers, as well as data transmission might be irregular from attacks. In cluster basis networks, data sensing, as well as transmission will consume sensor node energy. The expenditure of data transmission is high-priced when compared to that of data processing. Hence the technique that intermediate node combines data and forwards it to base station is chosen than method that each of the sensor node forwards data towards base station [6]. A sensor node will switch to sleep mode for the purpose of energy saving when it does transmit data, based on time-division multiple access control that is used for transmission of data.

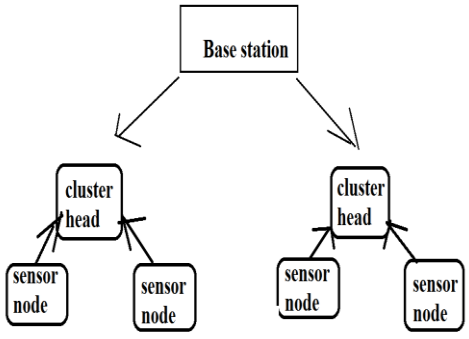

Fig1: Cluster Network

4. CONCLUSION:

Many wireless systems are organized in neglected and physical environments for assured applications. Secured transmission of data is the most serious issues for wireless systems. By means of the clustering approach, system performance of sensor networks was improved and data transmission based on clusters were examined by researchers for attaining of network management that improves node lifetime as well as decrease bandwidth consumption by means of usage of local collaboration between sensor nodes. We make a study of data transmission approach which is novel and effective for cluster-based networks in which clusters are produced dynamically. The approach of online or offline digital signature that is Identity-based was proposed to decrease storage expenses of signature processing. It may be efficient for key management in wireless systems and particularly offline phase is implemented on sensor node while the online phase is implemented throughout communication. Our work will suggest two data transmission approaches known as Identity-basis digital signature and online or offline digital signature scheme that is Identity-based were proposed for cluster based sensor networks. In the proposed protocols, secret keys along with pairing parameters are distributed in the entire sensor nodes by means of base station initially, that overcomes the problem of key escrow. Identity-basis digital signature as well as online or offline digital signature scheme that is Identity-based confirm the encrypted sensed information, by means of application of digital signatures towards message packets, that are competent in communication and apply the key management in support of security.

REFERENCES

[1] 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.

[2] 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.

[3] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[4] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229, 2001.

[5] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.

[6] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC), pp. 310-324, 2003.