IJARES/November 2015/Volume-3/Issue-11/2130-2135 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

ESTIMATION OF CLUSTERING METHOD PERFORMANCE FOR SENSOR NETWORK

G.Nuthan Kumar[1], B.Sunil Srinivas[2], D.Koteswararao[3]

[1]M.Tech Student, Dept of CSE, Vidya Vikas Institute of Technology, Chevella, T.S, India

[2]Associate Professor, Dept of CSE, Vidya Vikas Institute of Technology, Chevella, T.S, India

[3]Associate Professor & HOD, Dept of CSE, Vidya Vikas Institute of Technology, Chevella, T.S, India

ABSTRACT:

In the recent times, the technique of identity-based digital signature was been developed as an important management in sensor networks for the purpose of security. Research works have studied cluster basis sensor networks in literature but executions of cluster-based design actually are difficult. In our work we employ transmission of data in a secured approach for cluster-based sensor networks in which clusters are dynamically and regularly created. Two protocols of data transmission were introduced in a secured approach for cluster-based sensor networks known as identity-based digital signature and identity-based online or offline digital signature approach. The proposed identity-based digital signature and identity-based online or offline digital signature validate encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication and apply key management in support of security. Both the schemes will solve orphan node difficulty in transmission of data by means of symmetric key management.

Keywords: Identity-based digital signature, Orphan node, Cluster basis sensor networks, Data transmission, Key management.

1. INTRODUCTION:

Wireless networks are deployed in adversarial environments for applications, such as sensing by trust less surroundings. Transmission of data in a secured approach is necessary in many such useful wireless networks. Cluster-based transmissions were studied by researchers to get network scalability that exploits node duration and decrease utilization of bandwidth by local cooperation between sensor nodes [1]. Low-energy adaptive clustering hierarchy method is an extensively identified approach to stabilize expenditure of total energy for cluster-based networks. Addition of security to Low-energy adaptive clustering hierarchy like methods is tough since they dynamically and regularly reorganize network's clusters. Hence for provision of effective and long-term node-to-node trust associations is not enough for these types of protocols. The studies on identity-based digital signature method, based on factoring integers from identity-based cryptography, derive an entity public key from information of identity. The identity-based digital signature of online or offline approach was proposed for reduction of computation of signature processing. This scheme might be useful for key management in wireless networks. Importantly, offline phase is implemented on a sensor node whereas online phase is to be performed at some point in communication. In our work we implement transmission of data in a secured approach for cluster-based sensor networks in which clusters are dynamically and regularly created [2]. We put forward two protocols of data transmission in a secured approach for cluster-based sensor networks known as identity-based digital signature and identity-based online or offline digital signature approach. Both the schemes will solve orphan node difficulty in transmission of data by means of symmetric key management.

2. METHODOLOGY:

In a cluster-based sensor networks every cluster have sensor node, considered as cluster head that combines data by means of leaf nodes in its cluster, and sends aggregation towards base station. Cluster-based transmissions were considered to obtain network scalability that exploits node duration and decrease utilization of bandwidth by local cooperation between sensor nodes. Transmission of data in a

secured approach is the most important concerns in wireless networks. The probability of managing of asymmetric key was shown in wireless networks in the recent times that compensate deficiency from application of symmetric key for security. We suggest two protocols of data transmission in a secured approach for cluster-based sensor networks known as identity-based digital signature and identity-based online or offline digital signature approach. The proposed approaches of identity-based digital signature and identity-based online or offline digital signature validate encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication and apply key management in support of security. In the projected protocols, secret keys as well as pairing parameters are distributed in each and every sensor node by means of base station initially, that overcome the problem of key. Identity-based digital signature of online or offline approach is projected to decrease computational overhead for security, in which security depends on stability of discrete problem of logarithmic. This approach was proposed for reduction of computation of signature processing and it might be useful for key management in wireless networks. Importantly, offline phase is implemented on a sensor node whereas online phase is to be performed at some point in communication [3][4]. Both the schemes of identity-based digital signature and identity-based online or offline digital signature approach will solve orphan node difficulty in transmission of data by means of symmetric key management. Communication in identity-based digital signature will depend on Identity based cryptography, where public keys are the information of user identity hence they obtain equivalent private keys devoid of secondary transmission of data, that is proficient in communication.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Wireless network comprised of distributed devices by means of sensor nodes to scrutinize physical or else environmental conditions. The individual nodes sense environments, process information, and send information to collection points. Transmission of data in a secured approach is the most important concerns in wireless networks. We implement transmission of

data in a secured approach for cluster-based sensor networks in which clusters are dynamically and regularly created and propose two protocols of data transmission known as identity-based digital signature and identity-based online or offline digital signature approach. The conventional schemes are not specially considered for cluster-based transmissions which obtain network scalability that exploits node duration and decrease utilization of bandwidth by local cooperation between sensor nodes. In a cluster-based sensor networks every cluster have sensor node, considered as cluster head that combines data by means of leaf nodes in its cluster, and sends aggregation towards base station. We adapt conventional identity-based digital signature scheme for cluster-based sensor networks by means of distributing functions to various sensor nodes. Identity-based digital signature method, based on factoring integers from identity-based cryptography, derive an entity public key from information of identity. The identity-based digital signature of online or offline approach was proposed for reduction of computation of signature processing. The proposed identity-based digital signature has a procedure initialization previous to deployment of network and function in rounds throughout communication, where setup phase and phase of steady-state in every round. We assume that the entire sensor nodes recognize starting as well as ending time of every round due to time management [5]. In identity-based digital signature communication depends on Identity based cryptography, where public keys are the information of user identity hence they obtain equivalent private keys devoid of secondary transmission of data, that is proficient in communication. The proposed digital signature of online or offline approach operates in the same way to identity-based digital signature which has a procedure initialization previous to network deployment and works in rounds at some stage in communication. Proposed digital signature of online or offline approach works throughout communication, and self-elected cluster heads are decided on basis of their local decisions, hence it functions devoid of data transmission in cluster head rotations. Identity-based digital signature of online or offline approach is projected to decrease computational overhead for security, in which security depends on stability of discrete problem of logarithmic [6]. The proposed approaches validate

encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication and apply key management in support of security. In projected protocols, secret keys as well as pairing parameters are distributed in each and every sensor node by means of base station initially, that overcome the problem of key.

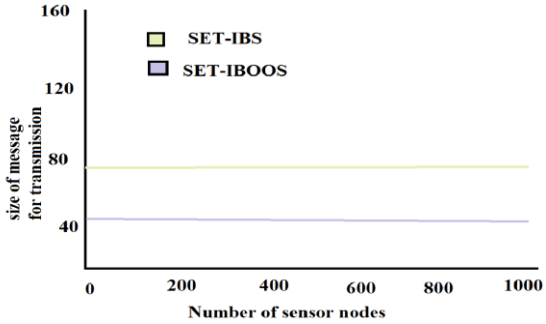

Fig1: Message size for transmission compared to nodes

4. CONCLUSION:

In the recent times, we have applied key management of identity-based digital signature to routing in cluster-based sensor networks. Data transmission in a secured means is the most important concerns in wireless networks. In our work we put into action transmission of data in a secured approach for cluster-based sensor networks in which clusters are dynamically and regularly created. Cluster-based transmissions were studied to get network scalability that exploits node duration and decrease utilization of bandwidth by local cooperation between sensor nodes. We propose two protocols of data transmission in a secured approach for cluster-based sensor networks known as identity-based digital signature and identity-based online or offline digital signature approach. The identity-based digital signature of online or offline approach was proposed for reduction of computation of signature processing. The proposed approaches of identity-based digital signatures validate encrypted sensed information, by means of application of digital signatures towards message packets that are competent in communication and apply key management in support of security.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

[5] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.

[6] 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.