ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on Networking: Wireless Sensor Network

Siddhant Nagarkar, Dr. R. V. Pujeri / Prof. Hanumant Pawar

Student, Department of Computer Engineering, MITCOE, Savitribai Phule Pune University, Pune, India

Assistant Professor, Department of Computer Engineering, MITCOE, Savitribai Phule Pune University, Pune, India

ABSTRACT: Advances in wireless sensor network (WSN) technology has provided the availability of small and low-cost sensor nodes with capability of sensing various types of physical and environmental conditions, data processing, and wireless communication. Variety of sensing capabilities results in profusion of application areas. However, the characteristics of wireless sensor networks require more effective methods for data forwarding and processing. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited. Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under these conditions. In this paper we are going to see some of the work done by several researchers on the topic.

I. Introduction

Wireless Sensor Network (WSN) is a distributed network and it comprises a large number of distributed, self-directed, tiny, low powered devices called sensor nodes alias motes. WSN naturally encompasses a large number of spatially dispersed, petite, battery-operated, embedded devices that are networked to supportively collect, process, and convey data to the users, and it has restricted computing and processing capabilities. Nodes are the small computers, which work collectively to form the networks. Nodes are energy efficient, multi-functional wireless device. The necessities for motes in industrial applications are widespread. A group of nodes collects the information from the environment to accomplish particular application objectives. They make links with each other in different configurations to get the maximum performance. Nodes communicate with each other using transceivers. In WSN the number of sensor nodes can be in the order of hundreds or even thousands. In comparison with sensor networks, Ad Hoc networks will have less number of nodes without any infrastructure.

Now a days wireless network is the most popular services utilized in industrial and commercial applications, because of its technical advancement in processor, communication, and usage of low power embedded computing devices. Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc. In many real time applications the sensor nodes are performing different tasks like neighbor node discovery, smart sensing, data storage and processing, to data aggregation, target tracking, control and monitoring, node localization, synchronization and efficient routing between nodes and base station.

Wireless sensor nodes are equipped with sensing unit, a processing unit, communication unit and power unit. Each and every node is capable to perform data gathering, sensing, processing and communicating with other nodes. The sensing unit senses the environment, the processing unit computes the confined permutations of the sensed data, and the communication unit performs exchange of processed information among three neighboring sensor nodes.

The sensing unit of sensor nodes integrates different types of sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors. The measured parameters from the external environment by sensing unit of sensor node are fed into the processing unit.

DOI: 10.15680/IJIRCCE.2017. 0501095

The processing unit is the important core unit of the sensor node. The processor executes different tasks and controls the functionality of other components. The required services for the processing unit are pre-programmed and loaded into the processor of sensor nodes. The energy utilization rate of the processor varies depending upon the functionality of the nodes. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors. The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit.

In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa**.**

II. RELATED WORK

In paper [2], authors have implemented a fully practical identity based encoded technique.given method has picked ciphertext security in the random oracle model reciving a modifyed computational Diffie-Hellman problem. Given system based on bilinear maps between clusters. The Weil mix on elliptic curve is a example of such a guide. They give a correct definition to secure identity based encryption schemes and give a couple of uses for such structures.

In paper [3], focus on efficient, data transmission conversing security in WSNs. More especially, they blend humble encoded methods with basic aggregation frameworks to fulfill greatly productive collection of encoded data. To evaluate the sensibility of proposed methodologies, they assess them moreover, show to a great degree promising results which doubtlessly exhibit calculable information exchange limit preservation and little overhead beginning from both encoded and aggregation operations.

In paper [4], authors developed an idea termed as Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recoup each sensing data delivered by all sensors regardless of the possibility that these data have been aggregated by cluster heads or aggregators. With these individual data, two functionalities are given. to start with, the base station can affirm the uprightness and authenticity of all sensing data. Second, the base station can perform any collection limits on them. By then, they propose two RCDA plans named RCDA-HOMO and RCDA-HETEfor homogeneous and heterogeneous WSN independently. They display that the proposed arrangements are secure under these attack demonstrate in the security investigation.

In paper [5], authors given one PH which can be shown secure against known-cleartext attacks, the length of the ciphertext space is much greater than the cleartext space. A couple of applications to assignment of touchy preparing and data and to e-betting are immediately sketched out. In the event that expansion is one of the cipher text process, by then it has been shown that a PH is unstable against a picked clear content attack. Consequently, a PH allowing full number juggling on encoded data can be most ideal situation secure against known-clear content assaults.

In paper [6], authors have given a strategy that 1) covers detected data end to end by 2) so far giving productive and adaptable in-network data aggregation. The aggregating intermediate nodes are not important to deal with the detected plain text data. They apply a particular class of encoded changes and talk about frameworks for enrolling the aggregate capacities "average" and "movement detection."

In paper [7], authors reconsider the relevance of additively homomorphic public key encryption counts for specific classes of remote sensor systems. Finally, they give proposals for selecting the most suitable public key plans for different topologies and remote sensor framework circumstances.

In paper [8], authors exhibit a novel kind of cryptographic plan, which engages any pair of customers to communicate securely and to check each other's marks without exchanging private or public keys, without keeping key indexes, and without using the administrations of a third party. The plan acknowledge the nearness of trusted key generation focuses, whose sole design is to give each customer an altered smart card when he first joins the framework.

D. Boneh and M. Franklin [9] given a short mark plan in view of the Computational Diffie-Hellman supposition on certain elliptic and hyper-elliptic bends standard security parameters, the mark length is about a large portion of that of a DSA signature with a comparative level of security. Our short mark plan is intended for frameworks where marks are written in by a human or are sent over a low-transfer speed channel. They studied various properties of our mark plan, for example, signature total and clump check.

V. C. Gungor observed in paper [10], that Minimizing force utilization is urgent in battery force restricted secure remote portable systems. In this paper, the author (a) present an equipment/programming set-up to measure the battery power utilization of encryption calculations through genuine living experimentation, (b) in view of the prowled information propose scientific models to catch the connections between force utilization and security, and (c) formulate and understand security augmentation subject to power imperatives. Numerical results are introduced to outline the increases that can be accomplished in utilizing arrangements of the proposed security boost issues subject to power requirements.

Table 1: Survey Table

Sr. No	Title	Paper Details	Method Used	Advantages	Disadvantages
1.	A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks	integrate a set of the cryptographic primitives into a SDA scheme in HSNs to achieve security requirements	practical SDA scheme	minimize energy consumption	---
2.	Identity-based encryption from theWeil pairing	ciphertext security in the random oracle mode	based on bilinear maps between groups	precised	---
3.	Efficient aggregation of encrypted datain wireless sensor network	intermediate sensors (aggregators) to aggregate the encrypted data of their children without having to decrypt them	provably secure additively homomorphic stream cipher	Provides stronger level of security	Identities of the non-responding nodes need to be sent along with the aggregate to the sink.
4.	RCDA: Recoverable concealeddata aggregation for data integrity in wireless sensor networks	recoverable concealed data aggregation	RCDA-HOMO	base station can securely recover all sensing data rather than aggregated results	Can cause additional costs
5.	CDA: Concealed data aggregation for reversemulticast traffic wireless sensor networks	principle suitability of symmetric additive PHs to aggregation functions average and movement detection	additive PH from Domingo-Ferrer	feasible	Does not support support of other PHs in CDA
6.	Public key based cryptoschemes for dataconcealment in wireless sensor networks	additive homomorphic public-key encryption schemes	encryption algorithms	reduc the energy consumption	data aggregation in untrusted
7.	Aggregate and verifiably encryptedsignatures from bilinear maps	aggregate signatures and constructed an efficient aggregate signature scheam	Key generation, aggregation, and verification	proved security	---

DOI: 10.15680/IJIRCCE.2017. 0501095

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

III. PROPOSE SYSTEM

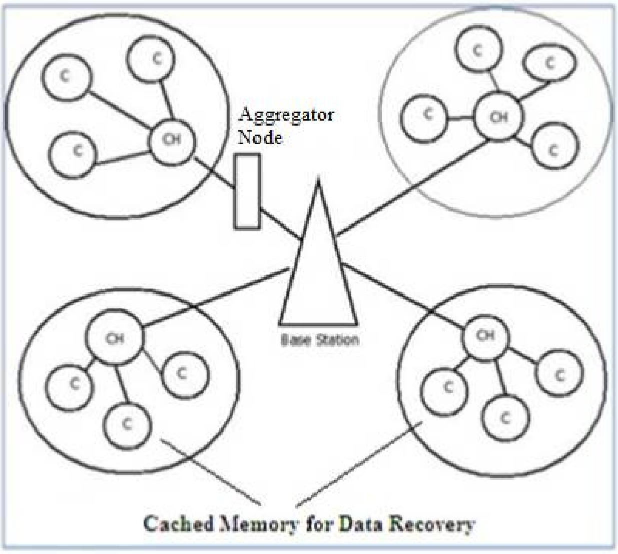

Fig 1. Propose System

IV. CONCLUSION

In this survey we have studied the some of the work done by the researchers on the topic of networking in Wireless Sensor Network detail also listed some their advantages and disadvantages. By this study we can conclude that there must be a system which will solve the issues in the present systems.

REFERENCES

1. Kyung-Ah Shim, "A Secure Data Aggregation Scheme Based on Appropriate CryptographicPrimitives in Heterogeneous Wireless Sensor Networks", in IEEE transactionson parallel and distributed systems, vol. 26, NO.8, august 2015.
2. D. Boneh and M. Franklin, "Identity-based encryption from theWeil pairing", SIAMJ. Comput., vol. 32, no. 3, pp. 586-615, 2003.
3. C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted datain wireless sensor network", MobiQuitous '05, pp. 1-9, 2005.
4. C.-M. Chen, Y.-H.Lin, Y.-C.Lin, and H.-M. Sun, "RCDA: Recoverable concealeddata aggregation for data integrity in wireless sensor networks," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 4, pp. 727-734, Apr. 2012.
5. J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism,"in Proc. 5th Int. Conf. Inf. Security, 2002, pp. 471-483.
6. J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reversemulticast traffic wireless sensor networks," in Proc. IEEE Int. Conf. Commun.,2005, pp. 3044-3049.
7. E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for dataconcealment in wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2006,pp. 2288-2295.
8. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. Int. Cryptol.Conf. Adv. Cryptol., 1984, pp. 47-53.
9. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encryptedsignatures from bilinear maps," in Proc. 22nd Int. Conf. Theory Appl. Cryptograph.Techn., 2003, pp. 416-432.
10. V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wirelesssensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557-3564, Oct. 2010.