Secure and Energy Efficient Routing in Wireless Sensor Networks: A Review

Nidhi Verma
CSE Department, Deen Bandhu Chhotu Ram University of Science and Technology, Haryana, India

Suman Sangwan
CSE Department, Deen Bandhu Chhotu Ram University of Science and Technology, Haryana, India

***Abstract*— Due to wide range of applications in current scenario, wireless sensor networks (WSNs) are gaining significant attention of researchers. Providing security and efficient energy utilization simultaneously in WSNs is a difficult task. Development of an energy efficient routing protocol has significant impact on overall stability and lifetime of sensor networks. WSNs may also be used for counterterrorism applications and infrastructure security hence security in such networks is a must. This paper will focus on analyzing existing techniques for enhancing the life time of sensor nodes and providing security at the same time in WSNs.**

Keywords—Wireless sensor network, Security, Energy Efficiency.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) drew consideration of researchers in different field in last few years. These networks are used for certain applications such as surveillance, traffic monitoring, seismic and acoustic detection and environmental monitoring etc. Main objective of clustering is to pass a solution that preserve stability between the sensors throughout the network operation. The major problem of research in distributed systems is energy consumption, a major part of research has been focused on study of algorithms and protocols that addresses these issues to resolve [1].

With the propagation of Micro-Electro-Mechanical System (MEMS) technology, WSNs have gained worldwide attention in recent year. MEMS has facilitated the development of the smart sensors. These are small and require limited computing and processing resources and these are inexpensive compared to traditional resources. Thousands of mini-computers fitted with sensors are deployed in a particular environment. These sensors can sense, measure and accumulate information from their environment and forward the sensed information to the user based on local decision processes. The sensors form a self-organized network and present the data after activation. The drift towards wireless-communication is progressively changing electronic devices in almost every area of life [2]. Sensor networks are the networks of small sensor nodes, it facilitate the analysis and monitoring of complex phenomenon over large areas and for long durations of time. A WSN is another type of ad-hoc network possessed of a large number of nodes that are fitted with different sensor devices. Small and inexpensive sensor nodes have been developed due to recent advances in sensor networks research, these sensor nodes can obtain expressive amount of data about physical values [3]. A wireless sensor network consists of spatially dispersed autonomous sensors that cooperatively supervise physical or environmental conditions. Each node in a sensor network is mainly equipped with a small microcontroller, an energy source (e.g. a battery) and a radio transceiver or other wireless communication device. Therefore these sensor nodes have variable cost, ranging from a few pennies to hundreds of dollars, depending on the level of complexity that is required by discrete sensor nodes and the size of the sensor networks. The size and cost coercion on sensor nodes results in analogous constraints on resources such as computational speed, memory, bandwidth and energy [4]. A sensor network is commonly a wireless ad-hoc network that means each sensor holds a multi-hop routing algorithm (such that so many nodes may transmit data in the form of data packets to the base station).

Conventionally, a WSN consist of thousands of low cost, small sized, low power sensor nodes. Sensor nodes usually communicate with each other via wireless transmission channels. These sensor nodes are arranged in an ad-hoc configuration to register physical phenomenon. Most wireless sensor networks are designed on the basis of ad-hoc network technology which maintains and coordinates a group of dynamic objects equipped with a transmission device in an area in which no fixed access points or base stations are present [5]. Despite the fact, ad-hoc network technologies are capable of establishing sensor networks, the use and design of sensor networks to supervise immobile nodes such as historic buildings, bridges and construction sites can be more interpreted to reduce overhead and power consumption. Direct transmission is the simplest approach for routing in wireless sensor networks, in this each node forwards its own data precisely to the sink. The cost of sending data to a

particular base station will become too high if that base station is too far away and the nodes will die quickly [3].

The growth of WSNs was motivated by military applications like battlefield surveillance. Many civilian and industrial application areas now uses WSNs, including machine health monitoring, industrial process control and monitoring, healthcare applications, habitat and environment monitoring, traffic control, home automation and scientific analysis in formidable environments [6].

The sensor nodes make use of its implicit battery for sensing and communication, in the occurrence of the battery's prostration, the sensor's utility completely halts, ineludibly leading to losing parts of the network utility, also changing the batteries of great number of sensor nodes over broad areas with possibly unsafe domain, like in military applications, or difficult to reach areas, like under water monitoring applications, is basically absurd. Therefore, so much research has centralised on maximizing the lifetime of the wireless sensor networks.

The analysis of the hotspot problem contrasts substantially whether the sink nodes or/and sensor nodes are mobile or not. If sink node is mobile as in, then the sink node will move in the vicinity of sensing area and gather data from the sensor nodes, thus adequately balancing the energy utilization in the WSNs. All the sensor nodes can forward the data systematically or save the data and hold-up the transmission of data till the displacement between the mobile sink node and the sensor node is nominal to decrease the power dissipation while holding-up data to the sink. If the sensor nodes are mobile, as in, the nodes can alter their location to help balance energy utilization in areas that have very high communication load or/and alleviate network distribution. Using sensor nodes and mobile sinks will raise the WSNs deployment cost. Also, in some applications mobility is absurd [7].

A network is divided into several clusters in hierarchical routing protocols. One node plays a leading role in each cluster. Communication with base station can only be performed by cluster-heads in the clustering routing protocols. Thus, routing overhead of normal nodes decreases significantly, because normal nodes have to forward the data to the cluster-heads only [1].

LEACH short for Low Energy Adaptive Clustering Hierarchy is the distributed clustering algorithm for routing in homogeneous sensor networks. Leach randomly elects the nodes cluster-heads and ascribe this aspect to several nodes according to round-robin management policy to assure fair energy dissipation among several nodes. The amount of data transmitted to the base station can be reduced if, the cluster-heads gather the data apprehended by the member nodes associated to their own cluster and then an aggregated packet is forwarded to the base station. We have two phases consisted by the protocol: First is the setup phase and second is the steady phase. Cluster-heads are selected in the first phase and then clusters are formed and data transmission to the base station takes place during second phase. In first phase, process of selecting cluster-heads is activated to elect future cluster-head. For networks arranged in large areas, LEACH is not advisable. Also, LEACH elects a list of cluster-heads randomly and there are no circumscriptions on their distribution and energy level [8].

For obtaining an efficient and faster solution of the clustering and routing problems, an analytical approach such as PSO (Particle Swarm Optimization) is greatly desirable. The considered PSO-based clustering takes care of consumption of energy of normal sensor nodes along with gateways. Particles are intelligently encoded to yield entire clustering solution for clustering. A different fitness function is also availed by taking care of those gateways which surely consumes more energy by acting as relay node in packet forwarding. Extensive simulation is performed on the proposed methods and evaluated with different performance metrics inclusive of number of active sensor nodes, network lifetime, total number of packet delivery, energy consumption, and so on [9].

Generally, sensor nodes behave as both data forwarders and data originators. Moreover, many-to-one communication pattern is followed by data transmission. Due to this, sensor nodes close to the sink have higher energy consumption as because they are loaded with abundant relay traffic. In these areas, sensor nodes tend to die early when they decrease their energy and it results in what is called as energy hole [10]. If this arises, no more data can be passed over to the sink, a reasonable amount of energy is emaciated and the network lifetime comes to a halt prematurely. Hence, the energy-hole problem should be considered for WSNs designing, along with node deployment. A novel deployment approach, called ACO (Ant Colony Optimization) is considered to resolve the problem of GCLC (Grid-Based Coverage with Low-Cost and Connectivity-Guarantee). Main goal of our approach is to decrease deployment cost, avoid the energy hole, to increase coverage speed, and then finally resolve the GCLC problem in a better way. ACO-greedy depends on the ACO (ant colony optimization), but it promotes ACO by adding a new aspect ants' greedy migration. It is an acclaimed intelligent algorithm in which complicated collective behaviour emerges from the ants' behaviour [11].

For securing data in WSNs, we must have encryption keys established among sensor nodes. Key distribution associates to the distribution of different keys between sensor nodes, and this is mainly a non-trivial security scheme. In authentication and data encryption, key management plays a central role. "Diffie-

hellmanand" is a security based on public key which is not appropriate for sensor networks because of resource constrains on sensor nodes [12]. Hence, using pre-deployed keying is the most efficient approach for bootstrapping private keys in sensor networks. In this case, keys are first loaded into sensor nodes and then their deployment takes place. Some works assert to manage the keys, which will be pre-deployed into sensor nodes, either in a probabilistic scheme or in a deterministic scheme. It is worth noticing that, techniques which are based on probabilistic scheme, should store an essential subset of keys for every sensor node. Also for having secure communication, sensor nodes need to interchange so many messages to see if they share the same key.

II. RELATED STUDY

In [13], a clustering algorithm was proposed which is used to increase the lifetime and scalability of the WSNs. For heterogeneous WSNs a distributed energy-efficient clustering algorithm is evaluated, which is Position-based clustering (PBC). This protocol is also called as an improvement of LEACH-E. It raises the lifetime of the whole network and performs function better than LEACH, LEACH-E and SEP.

In [7], power-aware routing was proposed in WSNs which focuses on the critical problem of increasing the lifetime of WSNs. A hybrid approach was used which combines two routing approaches, hierarchical multi-hop routing and flat multi-hop routing. The former aims to decrease the amount of traffic by utilizing data compression and the latter attempts to minimize the total power consumption in the network. This extend the lifetime of the network by mitigating the hotspot problem.

In [14] a Fuzzy logic approach was used and the proposed protocol contributes better stability period, lower instability period and higher energy efficiency as compared to LEACH protocol in spite of overhead of selection of master cluster head. A relevant master cluster-head selection can greatly enhance the lifetime of the network and drastically reduce the energy consumption.

In [11] it was explained that the most crucial issue in WSNs is node deployment because it concludes the detection capability of the networks, deployment cost and even the network lifetimes. A novel deployment approach, ACO-Greedy is proposed. This ACO-Greedy approach is based on the ant colony optimization including greedy migration mechanism, this decrease the deployment cost and complete the full coverage. Additionally, ACO-Greedy can adjust the communication/sensing radius to mitigate the energy hole problem and increase the network lifetime.

In [9] it was described that energy efficient routing and clustering are two acclaimed optimization problems which have been examined widely to enhance lifetime of the WSNs. Pratyay presents Nonlinear/Linear Programming (NLP/LP) formulations of these problems proceeded by two proposed algorithms for the same based on PSO (particle swarm optimization). A routing algorithm is developed with an efficient multi-objective fitness function and particle encoding scheme. The clustering algorithm is bestowed by considering energy conservation of the nodes via load balancing.

In [15] it was described that WSNs are ad-hoc networks consists of mainly small sensor nodes with limited resources (low bandwidth, low power and low storage and computational capabilities) and base stations (BSs). The sensor nodes aggregate data from surrounding environment and after processing transmit it to the base station (BS). Each and every sensor node has limited amount of energy and in most of the applications replacement of energy sources are not possible. LEACH is a clustering based protocol that uses a random-rotation of cluster heads. Simulated annealing optimization technique can be used to form clusters and cluster head rotations.

In [16] a key management technique SecLEACH was proposed which is based on random key pre-distribution. It provides secure communication between CH-node in LEACH. It also protects the network from outside attacks.

In [17] a LEACH-based key management was proposed which is based on Exclusion Basis System (EBS). It decreases the storage requirements of storing keys and reduces network communication load for updating cluster keys. Collusion attack may occur in EBS.

In [18] an efficient and secure key management scheme was proposed which is based on one way hash-function, data encryption and MAC. It provides continuous authentication of nodes in the network and reduces memory overhead. It has one disadvantage that it cannot deal with the malicious nodes.

In [19] a key management technique named Solar Aware Distributed LEACH protocol was proposed which is based on ECC and AES cryptography. It protects the network from attacks such as spoofing, selective forwarding, Sybil, hello flooding. In this solar powered nodes are selected as cluster head which is a disadvantage.

In [20] a security node based technique was proposed which is based on pair-wise key and cluster key. It provides more collaborative authentication security for key and it consumes less energy. It has strong resilience against node capture and can support large scale network. Its disadvantage is that it is applicable only on static networks.

In [21] a novel key management scheme for dynamic WSNs was proposed. It is based on Self-balanced binary search tree. This scheme has smaller memory and it only consider dynamic WSNs.

In [22] a DKS-LEACH was proposed. It was based on deterministic key distribution approach. It provides authentication, integrity, confidentiality and also minimizes memory usage. It consumes more energy.

TABLE I. Comparison of Various Techniques for providing energy efficiency and security in WSNs

S.No	Title of the Paper	Key Management Technique	Based On	Advantages	Disadvantages
1	SecLEACH–A Random Key Distribution Solution for Securing Clustered Sensor Networks	SecLEACH	Random Key Pre-distribution	Secure CH-node communication in LEACH and protects the network from outside attacks	Resilience is less
2	LEACH-Based Security Routing Protocol for WSNs	LEACH-based Key Management	Exclusion Basis System (EBS)	It decreases the storage requirements of storing keys and reduces network communication load for updating cluster keys	Collusion attack may occur in EBS
3	Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks	Efficient and Secure Key Management Scheme	One way hash function, data encryption and MAC	Provides continuous authentication of nodes in the network and reduces memory overhead	Cannot deal with malicious nodes
4	A Security Framework for Wireless Sensor Networks	Solar Aware Distributed LEACH protocol	ECC and AES cryptography	Protects the network from attacks such as spoofing, selective forwarding, Sybil, hello flooding	Solar powered nodes are selected as Cluster head
5	An Energy-efficient Security Node-based Key Management Protocol for WSN	Security Node based Key Management	Pair-wise key and cluster key	Consumes less energy, provides more collaborative authentication security for key, has strong resilience against node capture and can support large scale network	Applicable only on static network and is not scalable
6	A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network	Novel key management scheme for the dynamic WSNs	Self-balanced binary search tree	This scheme has smaller memory	Only dynamic WSNs are considered
7	A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks	DKS-LEACH	Deterministic key distribution approach	Provides authentication, integrity, confidentiality and also minimizes memory usage	Energy consumption is more

III. CONCLUSION

This paper has focused on significant work done by researchers till date for providing security and efficient energy utilization in WSNs. The work has been summarised in Table I. A plenty of research has been accomplished on supplying security to WSNs but little work has been done on reducing energy consumption while providing security. Future work will focus on proposing a technique for increasing WSNs lifetime and providing security at same time.

REFERENCES

[1] Salim EL Khediri, Nejah Nasri, Anne Wei, Abdennaceur Kachauri, "A New Approach for Clustering in Wireless Sensors Networks Based on LEACH", International Workshop on Wireless Networks and Energy Saving Techniques (WNTEST), Procedia Computer Science 32 (2014) 1180 – 1185.

[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey", Computer Networks 52 (12) (2008) 2292–2330.

[3] Jeong-Hun Lee, Ilkyeong Moon, "Modeling and optimization of energy efficient routing in wireless sensor networks", Applied Mathematical Modelling 38 (2014) 2280–2289.

[4] I.F. Akyildiz, W.S.Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Commun. Mag. (2002) 102–114.

[5] O. Salami, A. Bagula, H.A. Chan, "Framework for link reliability in inter-working multi-hop wireless networks", Math. Comput. Modell. 53 (11–12) (2011) 2219–2228.

[6] D. Wagner, R. Wattenhofer, "Algorithms for Sensor and Ad-hoc Networks", Springer-Verlag, Berlin Heidelberg, Germany, 2007.

[7] Ahmed E.A.A. Abdulla, Hiroki Nishiyama, Nei Kato, "Extending the lifetime of wireless sensor networks: A hybrid routing algorithm", Computer Communications 35 (2012) 1056–1063.

[8] W. R. Heinzelman, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensors networks", IEEE transaction on Wireless Communication, 2002.

[9] Pratyay Kuila, Prasanta K. Jana, "Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach", Engineering Applications of Artificial Intelligence 33 (2014) 127-140.

[10] Cheng Tien Ee, Ruzena Bajcsy. "Congestion control and fairness for many-to-one routing in sensor networks", In: Stankovic JA, Arora A, Govindan R, editors. Proceedings of the 2nd ACM conference on embedded networked sensor systems. Baltimore, US: ACM Press; 2004.

[11] Xuxun Liu, Desi He, "Ant colony optimization with greedy migration mechanism for node deployment in wireless sensor networks", Journal of Network and Computer Applications 39 (2014) 310–318.

[12] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys, vol. 8, pp. 2–23, 2006.

[13] Abderrahim Beni Hssane, Moulay Lahcen Hasnaoui, Mostafa Saadi, Said Benkirane, "Position-Based Clustering: An Energy-Efficient Clustering Hierarchy for Heterogeneous Wireless Sensor Networks", International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 2831-2835.

[14] Tripti Sharma, Brijesh Kumar, "F-MCHEL: Fuzzy Based Master Cluster Head Election Leach Protocol in Wireless Sensor Network", International Journal of Computer Science and Telecommunications, Vol. 3, Issue 10, October 2012.

[15] Gauri Bajaj, "Leach Enhancement Using Simulated Annealing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015.

[16] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro, "SecLEACH–A Random Key Distribution Solution for Securing Clustered Sensor Networks", NCA '06 Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications, IEEE Computer Society Washington, DC, USA ©2006, Publication Date: 24, July 2006, 145-154.

[17] Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian, "LEACH-Based Security Routing Protocol for WSNs", D. Jin and S. Lin (Eds.): Advances in CSIE, Vol. 2, AISC 169, pp. 253–258.

[18] Abdoulaye Diop, Yue Qi, Qin Wang, "Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks", I.J. Computer Network and Information Security, 2014, 8, 9-18.

[19] Namdeep Singh, Er. Jasvir Singh, "A Security Framework for Wireless Sensor Networks", Journal of Global Research in Computer Science, Vol. 4, No. 7, July 2013.

[20] Bi Jiana, E Xu, "An Energy-efficient Security Node-based Key Management Protocol for WSN", Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13), Published by Atlantis Press, Paris, France. © the authors, 2013 0062.

[21] Sai Ji, Liping Huang and Jin Wang, "A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network", International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013.

[22] Mandicou Ba, Ibrahima Niang, Bamba Gueye and Thomas Noel, "A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks", Published in Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on 11-13 Dec. 2010, 422-427.