International Journal of Computer Science and Engineering Communications
Volume 7, Issue.1 (2019) Page.1855-1860
www.ijcsec.com

Improve Energy Consumption in Wireless Sensor Networks Through Secure Clustering

Ahmad Aminibar
Department of Computer and Information Technology,
Qaemshahr Branch, Islamic Azad University, Qaemshahr, Iran.
Email: ahmadaminibar@yahoo.com

Abstract: *Recent advances in MEMS systems, intelligent sensors, wireless communications, and digital electronics make it possible to build small, low-power, low-cost sensor nodes that can communicate wirelessly. These tiny sensor nodes consist of three sensor parts, data processing, and wireless data transmission. In general, a wireless sensor network contains a large number of these nodes. For measuring a parameter, their data are considered collectively. In wireless sensor networks, sensor nodes with a large number of intrinsic or very close to target sensors are used to measure the parameter. Sending data by clustering improves quality and reduces energy. Along with the transmission of information, its security should also be considered. In the proposed scheme, the Distributed Fault-Tolerated Clustering Algorithm (DFCA) and the Elliptic Curve Distributed Sign Algorithm (ECDSA) are used. The ECDSA algorithm is handy for the wireless sensor network because of its simplicity and low overhead.*

Keywords:*Wireless Sensor Network, Clustering, DFCA, ECDSA, Security*

Citation: Ahmad Aminibar. **"**Improve Energy Consumption in Wireless Sensor Networks Through Secure Clustering." *International Journal of Computer Science and Engineering Communications* 7.1 (2019): 1855-1860.

I. INTRODUCTION

Sensor nodes have limited processing and storage capacity, so they can only perform limited computing operations. These hardware constraints create many challenges in software development and network protocol design for sensor networks, so that not only must the energy constraints In sensor nodes, it is necessary. The processing and storage capacities of the sensor nodes are considered [1]. Wireless sensor networks include a large number of low-cost, low-cost nodes that connect through a wireless network that collects data locally through a multicast wireless transmission [1]. The number of sensor nodes is several times the number of nodes in the wireless network. Sensor nodes are often used without detailed and planned planning, so they should be able to organize themselves in a communications network. A Wireless Sensor Network (WSN) includes a multiple sensor that is capable of compromisingly low power and computing power.

A sensor in each cluster acts as a cluster and has cluster management and cluster access applications. The sensors in the network can be grouped into clusters, each of which is controlled by a special sensor known as a cluster head. All sensors in a cluster communicate with clusters that act as a local sink. The inherent nature of wireless sensor nodes, such as resource constraints, are easily captured and possibly manipulated. Sensor nodes of the wire make the security plans designed for network-based wireless networks unacceptable for wireless sensor networks [2].
The energy consumed by the sensor nodes for processing operation is negligible and unobtrusive compared to the energy consumed for transmitting and transmitting data. Data transfer consumes the most energy compared to data calculations [3]. All security services use a limited amount of sensors and they consume more energy. For higher security purposes, prevention of multiple attacks is essential and requires more energy and the main forms of performance are high energy consumption. Reducing energy consumption is the most important goal in designing a sensor network. Energy consumption is performed across all network nodes. In order to maintain and save energy, when there is data to report in some parts of the network, only a subset is needed. The sensors are active [4].
Secure clustering and key hosts have problems with wireless sensor networks. Therefore, an efficient management key should be designed to distribute cryptographic keys among sensitive nodes. Each safe clustering program identifies a threat model from attacks before the attack, and offers solutions to prevent resistance to them [5]. Confrontation with these types of attackers is based on decoding secure clustering techniques. In order to design an effective security solution, the attackers and their impact on clustering needs to be identified. Invaders may acquire cluster and cluster members (CH) information from the clustering process. An attacker may cluster into clustering in the cluster setup phase, or to prevent clustering of some nodes. A clustering method should safely identify and retrieve these nodes, although having these properties is appropriate in a clustering scheme, but for one A complete security system is not enough. Safe cluster designs and wireless sensor networks try to enhance security features of clustering algorithms and prevent malicious behaviors and disrupt the process of creating and maintaining clustering [5].
Invaders may interfere with communication between the cluster header or the cluster and sensors by launching DOS or attacks. In a cluster-based network, cluster headers are more important targets for attack because cluster-based protocols rely on cluster headers to aggregate data and traffic. Blocks are attacked, by sending selectively, sinking wells and sending data Fake, attacking the network [6]. To design sensor network protection from malicious attacks, it's very difficult to design security mechanisms or protocols that are both energy efficient and powerful in terms of security [6].

II. REALTED WORKS

As the leach of the sensor nodes at the closest gate and each gate makes its clusters, after the completion of the formation of a stable phase cluster, in which the gates begin to receive data from the cluster sensor nodes they They collect the tubes using the Tdma planning to the base station [7]. For more secure security, trust-based hybrid methods relate to leaching cryptographic and trust methods that protect traffic inaccessible attackers. You must identify the data transmitted or the source of the data, but there are no proposals for The leach protocol is unknown [8]. The non-cluster head node chooses a cluster with respect to the ch energy, and the ch from the chassis, eventually the CH uses the multimode transfer data to the BS.
Leach-D was found to reduce overall network power consumption [9]. The energy savings result of a sensor node is that node nodes send a cluster of their data to their cluster group, which is more likely to send a cluster It is to the base station [7]. One can use a lower power node to carry

out the sensor work and send the sensed data to the cluster head in a short time. To reduce the data transferred to the sink, and to increase network performance, aggregation of data in cluster headings can be divided into two single-cluster architectures or several fragmentation. In a network, the multi-hierarchy of cluster-based hierarchical network architectures can not only reduce energy consumption for communications, but also can balance traffic load and provide scalability while growing network size.

III. THE PROPOSED METHOD

In DFCA, whenever the gateway of each cluster is dead, the encryption based on wireless sensor networks using ECDSA makes sensor nodes near the sink to consume more energy than other nodes and increase energy consumption.All cluster nodes and gates are deployed manually or randomly in a sensitive area and then fixed and expanded. Each cluster will be connected to a gateway alone. If the gate is within the communication range of the sensor node, the gate They are able to communicate in a long way with sensor nodes and can communicate with the BS. The wireless links are symmetric so that a node can calculate the approximate distance to another node based on the received signal strength. Clusters that have at least one gate in their communication range. A set of cover covers of all nodes covered in WSNs. Unknown nodes are sensor nodes that have no gate in their communication range. All cluster gates are placed under the bootstrap process. In the DFCA, the ACT protocol uses the energy consumption network topology to calculate the cluster radius to balance the energy dissolution of each CH. The ACT protocol is intended to guarantee the security of any gateway gateway in the WSN through ECDSA. Because of uncertainty in the WSN environment, the key management uses the ACT protocol to make a decision effectively. In DFCA, public key cryptanalysis can provide a high level of security with reasonable expense in the WSN using ECDSA.

In DFCA, gates are more energy than nodes they are normal and are known as cluster heads. This limitation in the DFCA has been eliminated by generating the maximum energy remaining nodes among all the passive nodes as new nodes of the cluster head transport to the base station using this new header cluster. In the DFCA, the active nodes of the cluster are connected to the neighboring gate Using this new gateway, they send their data to the base station. Sensor nodes can be assigned to both devices if they are within the communication range of the sensor node. Therefore, the gateways can collect sensor data and ultimately transmit local network information to the base station. In DFCA, the main role of the cluster is to collect all collected data from the nodes and to eliminate the data that is lost. This will allow the base station to retrieve information through ECDSA to improve data security. In the DFCA, gateways have more energy than normal nodes and are known as cluster headers. These special nodes also have a battery and therefore have a limited time. A sensor node detects the surrounding gates based on the remaining gate energy of the node to the gate and the gate The DFCA selects the base station's unique identity to all nodes, including gateways on the network. In the ECDSA, digital signature of the elliptical curve can be calculated by the gateways in the message. ECDSA creates clusters Which improves energy consumption in wireless sensor networks. During ICP clustering, when the sink sends a query to aggregate data, the energy is mainly calculated by message exchange, and each source sensor that holds the appropriate data by sending data to the sink via the ECDSA as Independent of other sensors. The clusters use the ECDSA for additional energy to minimize the number of clusters. This causes clusters to separate more and require less cluster noise than the same number of nodes Cover a little. Single-digits use the ECDSA with the public key for gates and the comparisons of the public key received by it. The ECDSA causes the node with a poor power status to have no chance of selecting the cluster so that the network is increased.

We use the ECDSA as a protocols for producing and typing signatures for key transfer. Several finite elements are used to create elliptical bending groups. In LEACH, sensor nodes are placed at the closest gate and each gate is made up of its own clusters. In LEACH, the cluster head changes after each other. Upon completion of the cluster, each CH sets the TDMA program for its member nodes, and adjusts this program It transmits its member sensor nodes. After the cluster is formed through ECDSA, each cluster heads the creation and distribution of the TDMA program among each of its clusters. LEACH uses nodes that are based on the base station to save energy. . In LEACH, due to the random selection of the cluster, it is possible that the selected cluster head has enough energy to transmit data to the E There is no base station and it does not go away. So all the information that goes into each of our clusters is destroyed. LEACH randomly selects nodes from node cluster and assigns this role to different nodes based on the Rolling Management policy to ensure that released energy between the nodes to reduce the amount of information transmitted to the base station of the cluster heads causes Collecting data taken by the element nodes belonging to the cluster itself and then sending a packet collected to the base station.

IV. EVALUATION

The primary energy of the sensor nodes is 2 jules and their number is 350. The primary energy of the gatway is 10, the number of them is 35, and the network dimensions and sink coordination are 300 to 300 and (150,150) respectively.

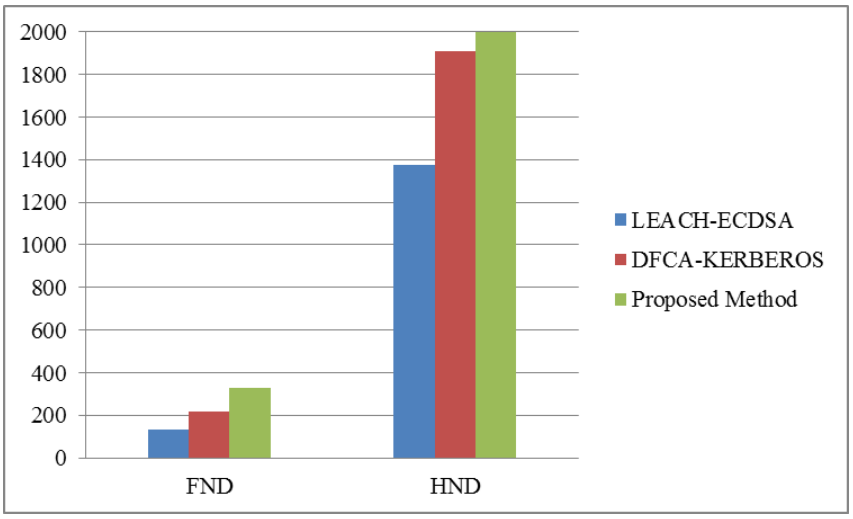

Fig. 1. HND and FND in the LEACH _ECDSA, DFCA_Kerberos and proposed

One of the most important parameters in the wireless sensor network is the network lifetime. Most of the methods and articles in the field of wireless sensor network have been used to prove the superiority of their method, which has increased network lifetime. Two measurements are usually used to measure network lifetime. The first node die (FND) is considered one of the most important criteria. This means the start-up time of the network until the first node that completely depletes the energy. The next criterion is the time interval between the start of the grid and the half node die (HND). Figure 1 shows the values of HND and FND obtained from the three LEACH-_ECDSA, DFCA_Kerberos and proposed methods. As you can see, the proposed clustering method is better in terms of HND and FND compared to LEAC _ECDSA and DFCA_Kerberos.

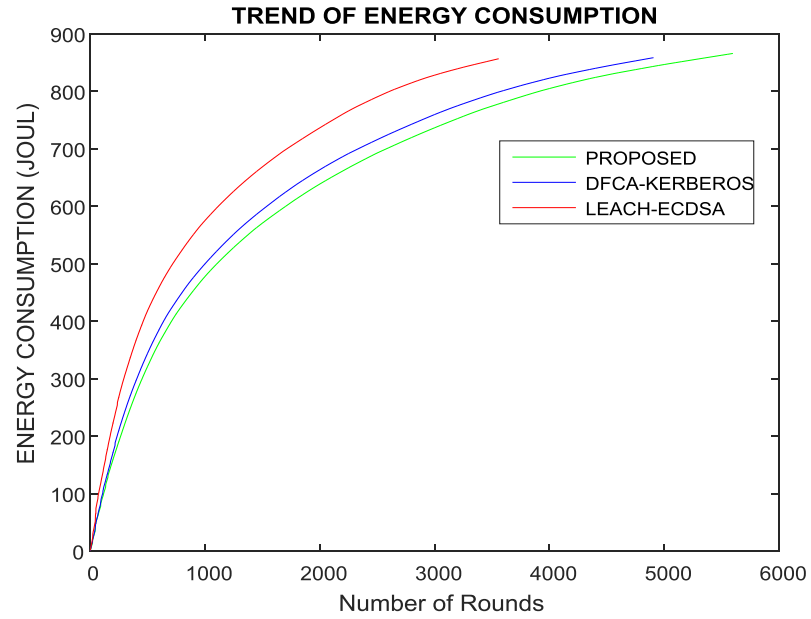

Fig. 2. Energy consumption

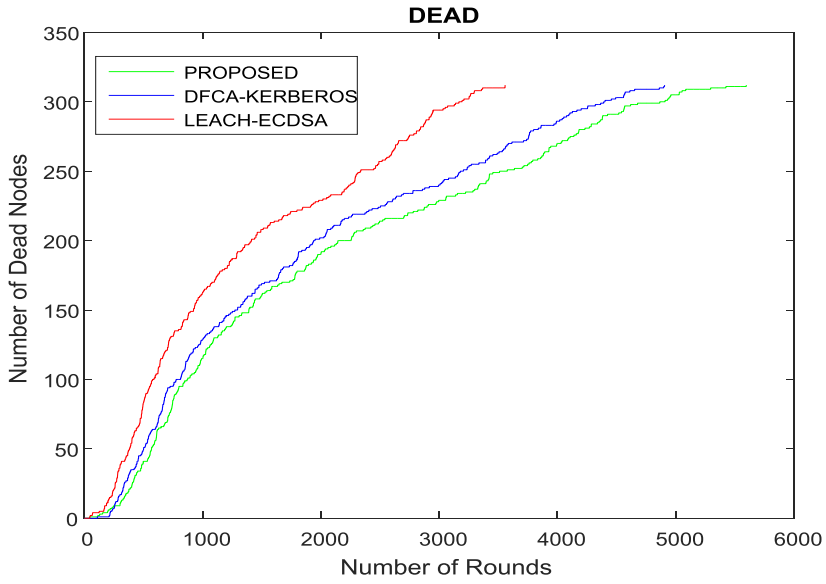

Fig. 3. The nodes' outage process

The graphs shown in Figures 2 and 3 indicate, respectively, the amount of energy consumed in each round of network execution and the nodes in each round. From these diagrams it can be concluded that in each round the number of nodes in the proposed method is better than LEACH-_ECDSA and DFCA_Kerberos. Also, the energy consumption in LEACH-_ECDSA and DFCA_Kerberos is higher in each round of the proposed method. In general, based on the criteria measured in this scenario, the proposed method has a better performance than LEACH_ECDSA and DFCA_Kerberos.

V. CONCLUSION

In this research, the problem of secure clustering in wireless sensor networks has been addressed with the aim of reducing energy consumption and maintaining network coverage.

To achieve this goal, a DFCA clustering algorithm was first used to propose an energy-based clustering protocol. This new protocol will make clustering according to the two remaining nodal energy standards and the distance between each node and the base station. Then, the data transmission between the clusters in the cluster with the cluster and between the cluster heads and the base station is secured with the ECDSA algorithm. Then, the superiority of the proposed method in terms of increasing the lifetime and maintaining the network coverage (by simulation) has been proven.

REFERENCES

[1] F.K. Shaikh, and S. Zeadally, Energy harvesting in wireless sensor networks: A comprehensive review, *Renewable and Sustainable Energy Reviews, 55,*2016, 1041-1054.

[2] J. Tan, A. Liu, M. Zhao, H. Shen, and M. Ma, Cross-layer design for reducing delay and maximizing lifetime in industrial wireless sensor networks,*EURASIP Journal on Wireless Communications and Networking, 2018(1),*2018, 38-50.

[3] X.Y. Liu, Y. Zhu, L. Kong, C. Liu, Y. Gu, A.V. Vasilakos, and M.Y. Wu, CDC: Compressive data collection for wireless sensor networks,*IEEE Transactions on Parallel and Distributed Systems, 26(8),*2015, 2188-2197.

[4] A.A. Mugheri, M.A. Siddiqui, and M. Khoso,Analysis on Security Methods of Wireless Sensor Network (WSN),*Sukkur IBA Journal of Computing and Mathematical Sciences, 2(1),*2018, 52-60.

[5] A.S. Rostami, M. Badkoobe, F. Mohanna, A.A.R. Hosseinabadi, and A.K. Sangaiah, Survey on clustering in heterogeneous and homogeneous wireless sensor networks,*The Journal of Supercomputing, 74(1)*, 2018, 277-323.

[6] S.P. Singh, and S. C. Sharma, Secure clustering protocols in wireless sensor networks,*Journal of Wireless Sensor Network, 3(1),*2016, 1-9.

[7] V.K. Arora, V. Sharma, and M. Sachdeva, A survey on LEACH and other's routing protocols in wireless sensor network,*Optik, 127(16),*2016, 6590-6600.

[8] R. Azarderskhsh, and A. Reyhani-Masoleh, Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks,*EURASIP Journal on Wireless Communications and Networking, 2011(1),* 2011, 893592.

[9] S. Tyagi, and N. Kumar,A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks,*Journal of Network and Computer Applications, 36(2),*2013, 623-645.

BIBLIOGRAPHY OF AUTHORS

Ahmad Aminibarwas born in Qaemshahr, Iran, in 1988. He received the B.Sc. degree in Information Technology Engineering from Payamnour University, Sari Branch, Sari, Iran, in 2014. He is currently M.Sc. student in Computer Engineering from Qaemshahr Branch, Islamic Azad University, Qaemshahr, Iran. His research interests include computer arithmetic and wireless sensor network.