Engineering Universe for scientific Research and management
ISSN (Online): 2319-3069
Vol. XIII Issue X
October 2021

A SURVEY ON COMMUNITY DETECTION ON SOCIAL MEDIA NETWORK

Tanvi Tomar[1], Chinmay Bhatt[2], Varsha Namdeo[3]
CSE, SRK University, Bhopal, India[1, 2, 3]
Tanutomar1309@gmail.com[1], chinmay20june@gmail.com[2], varsha_namdeo@yahoo.com[3]

ABSTRACT: In wireless sensor networks (WSNs), the energy supply of sensor devices is limited. One of the basic architecture problems in WSNs is sensor dies due to dissipating battery capacity. As a result, it is argued that energy conservation is the most significant criterion for any protocol built for WSNs. Thousands of lightweight, inexpensive sensors can be randomly distributed in open and harsh environments to gather data in Wireless Sensor Networks (WSNs). The low battery life of battery-operated sensors, as well as hostile conditions, requires the development of energy-efficient, secure and reliable sensor network protocols. Routing, out of the broad range of network protocols, is the most critical in terms of energy consumption, as data transmission absorbs 70% of total energy in WSNs. As a result, energy-efficient routing systems must be built in order to save energy and increase the network's lifespan. However, resource-limited sensors, the lack of a global solution scheme and the application-specific nature of WSNs pose a challenge to routing. Furthermore, security is yet another critical problem in WSNs, as sensors are typically installed in insecure areas and susceptible to security attacks. Many of the current routing protocols have various security measures in place to meet security objectives. We present a brief review on various secure and energy-efficient routing protocols in wireless sensor networks, outlining their underlying principle and operations.

Keywords: Wireless Sensor Networks, Routing Protocols, Energy Efficient Protocols, VANET, ADHOC

1. INTRODUCTION

WSNs are promising a promising technology due to their broad range of applications in environmental monitoring, industrial use, military utilities, and civil domains like IoT and smart home applications. Wireless networks have many restrictions imposed on sensor nodes on energy resources, processing power, and storage, which are not commonly found in other traditional networks like MANET or VANET. The aims of WSN are to deploy sensor devices in nodes in distributed manner randomly in unattended and remote areas which locations are remotely monitored. In those remote locations the adhoc nature of WSN offers the connectivity there wirelessly. The characteristics of sensor nodes and the ad-hoc networks, such as decentralized in nature and need of less infrastructure, in WSN gives the potential to fulfill need of low-cost solutions. All WSNs are designed specifically according to their applications, in which specially chosen nodes with desired sensors, are deployed according to the best suitable topology. These nodes sense information from surroundings and send this information via carrier links to base station, where this information is consumed for the application.

In recent years, WSN has been considered as major communication support to the environmental monitoring systems, industrial monitoring, security surveillance and automation control purposes. This stimulating importance makes WSN an inviting research field for academicians as well as industries for better communication solutions with promising QoS (Quality of Service) [1], energy efficient, secure,

reliable communication needs. Sensor nodes are tiny devices which monitor the conditions like humidity, temperature, pressure and then later convert them into electrical signals. The communication is either directly between the base system and sensor, or among the sensor nodes. These nodes are programmable and used together to get data from various environments. Sink nodes [2] are targeted to get data from all surrounding nodes and source nodes are targeted to collect the data from environment.

The sensor nodes are backbone and important part of the wireless sensor networks because all wireless sensor network is comprised of the nodes, the only external part is base station which is responsible for handling all the data which is produced by the sensor nodes in wireless sensor network. Sink node plays a vital role because all collected data is forwarded to the sink node, and sink node forwards this data to the base station. The basic idea of wireless sensor network is to distribute the small sensing devices, which can sense some changes in the parameters and communicate with other devices, over a defined Geographic area. This defined area is the area in which a wireless sensor network is deployed and is operational. The monitoring of this wireless sensor network is done by the nodes itself [3] and the mechanism deployed inside the nodes. The nodes are usually simple and low cost because of economic and operational limitation. They are often unattended, so they are likely to suffer from various types of attacks.

2. ARCHITECTURE OF WSN

WSN architecture includes the hardware architecture and the network architecture. In hardware architecture we consider the sensor node architecture and in network architecture the architecture of the communication or way of the communication is considered.

2.1. Sensor Node Architecture:

The sensor node architecture is consisting of these major components: sensors, small Processing Unit, which is composed of processor & memory, a transceiver unit consist of transmitter & receiver and a small battery (power unit) which can supply power to this sensor node. The architecture of sensor node [4] depends upon the application of that wireless sensor network, so in some applications the sensor node optionally may have any Location Finding System (for example GPS) or a mobility controller or mobilize unit as shown in figure 1.

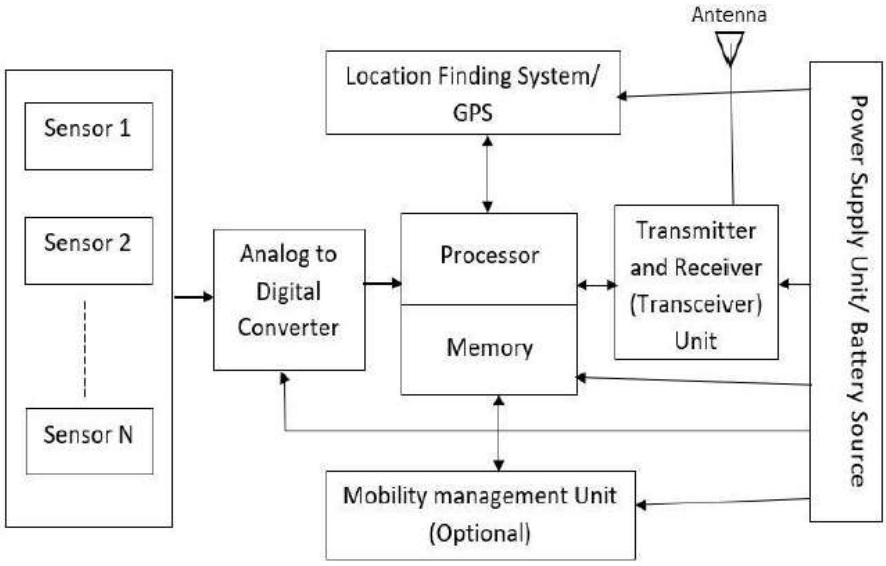

Figure 1: Sensor Node Architecture

Also depending on the application and place of deployment the wireless sensor network, these nodes may be connected to the power supply or solely dependent on the small battery which be fixed with these sensor nodes.

2.2. Communication Architecture:

Communication architecture of WSN consists of the scattered nodes structure and specific geographical area, with each of these nodes is capable of collecting

and sending the data back to the sink or to the base station or end users specified in the scheme. The communication structure of WSN has 5 standard layers which are from top to down as follows [5]: Application layer, Transport layer, Network layer, Data Link layer and Physical layer. It also has 3 management planes: 1) power management plane, 2) mobility management plane and 3) task management plane. Following figure 2 shows the five layers and three planes of WSN communication architecture. The details shown in figure 2

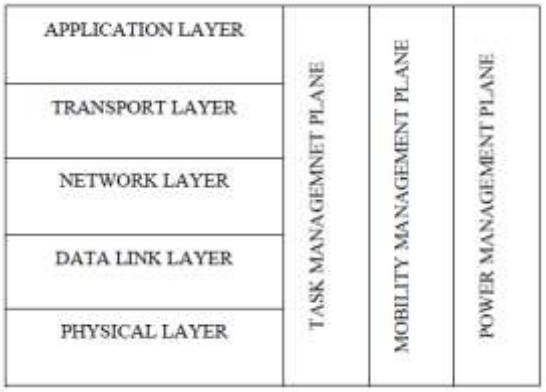

Figure 2: Communication Architecture

3. ROUTING PROTOCOLS FOR WSN

Data is efficiently transferred around WSNs between the spatially distributed nodes and sink nodes intermittently. Due to its unrealizable link with a computer, the sorting of the nodes in WSN cannot satisfy the need for all applications with a single routing protocol. Many routing protocols have been studied, according to the features of grouped applications. These protocols will typically be categorized for five classes [7]: flood routing protocol, hierarchical and data-centred routing protocol, location-based routing protocol and the routing protocol based on QoS as shown in figure 3.

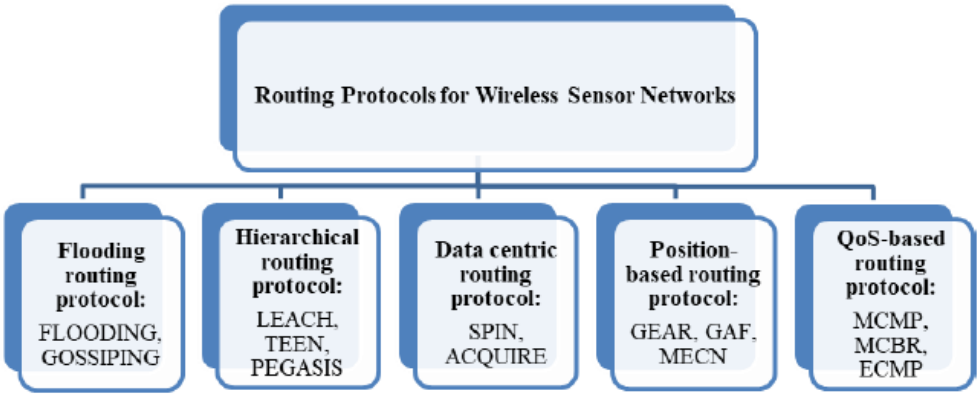

Figure 3: Conceptual Classification of Routing Protocols in WSN

3.1. Protocol for Flooding Routing

This may be the companion for the past protocol for routing. It takes little time to keep up the system and routing and the data receiving node legally can broadcast the data pack to a nearby nodes. The flooding mechanism is also an elevated rapid procedure, but the

messages "implosion" and "broadcast" should be properly used by the companion system. Inefficiency is not considered as it is a helpless side of resource limitations.

Flooding routing protocol: Flooding will probably entail the progress of the mill flow path. To carry out routing it does not need to preserve the topology structure of the network. One data accepter can transfer data packets in a given structure to any or all nodes. For short messages and tinny data sets this strategy is good. But this strategy has the chance that nodes may be dead before the data transmission completes towards its target or makes the most absurd choice for routes. So, it gives very low energy efficiency and performance in case if we a large set of data to transfer.

3.2. The Hierarchical Protocol

The basic concept of such a protocol is to link nodes for a network path. The cluster head nodes will collect and aggregate data in order to decrease transmission costs of all nodes and transfer aggregated data to the sink node at the last moment. This mode can be used to assess the WSN adaptability and to use the WSN nodes to increase the network lifetime.

Hierarchical protocol for routing: the LEACH protocol is widely liked in WSN routing and most used clustering protocol. LEACH has been extended into several variations by modifications in the existing protocols. The main purpose of the protocol is to carelessly and impartially pick a cluster head node to share the hand-off correspondence of wireless devices in order to continuously consume the power of nodes during the intermediate periods when the gadget consists and postpones the network lifecycle longer. This protocol has two steps: the preparation stage of the cluster and the arranging of data transfer.

A round is assumed to be the sum of times of these two phases. A cluster head is chosen unpredictably as a center in the package availability sorting. The cluster head node sends messages to nature and, in general, entirely different node groups choose a cluster to participate, according to the strength of the transmission message they have and currently send the corresponding bundle heads. A cluster head communicates thoroughly with a sink node, so the clusters communicate in their own groups with the cluster head.

LEATCH (Low Energy Adaptive Tier Clustering Hierarchy) [8] offers solutions to the coverage problems that LEACH has faced and is eventually succeeding in proposing better performance, less latency, and lower power consumption than LEACH has achieved. LEATCH implements the enhanced LEACH mechanism to minimize energy consumption, expand the network coverage, increase scalability and reduce latency. In this approach LEATCH proposes more than one clustering stage in hierarchical manner for WSNs to ensure better connectivity between the Base Station and most nodes. TEEN protocol: TEEN includes a specific reactive mode, but the cluster head nodes form a hierarchical structure that is subject to the partition between them, which directly or indirectly communicate to the sink nodes. The CH allocates time slots to nodes to transmit their data. CH collects data from nodes and then fuses that as common data stream with the interim characteristic of recognition. Only CH must fuse the data and thus it is energy saving for nodes. PEGASIS protocol: LEACH is upgraded by the PEGASIS protocol. The node in PEGASIS only talks to the nearest node that is closest to maintaining a significant saving from a lot of overhead communication over cross-section corrections by having a cluster head guarantee.

3.3. Data Based Routing Protocol

As a name, the information inside the indicator should be established by means of a specific technique of representation. The transmission of data is based on the request for information and on the naming of information. Most exchanges of learning are held on the local level. These interactions will never again be based on a single node, but will focus on learning within this system, thereby reducing the complexity of repetitive and terrible knowledge conveyed in a frame from top to bottom, saving needless overhead and postponing the cycle of life.

Data-Centred routing protocols: The data in the network compose a fussy representation system in this form of protocols. The transmission of data is based on the request for information, as well as on naming information. Most information shared is stored locally. Therefore, connectivity depends less on a certain node but more on information within the network.

Sensor Protocol for Information via Negotiation (SPIN): This method is designed to eliminate flood and

gossip vulnerabilities. The idea is to use more tools than metadata to exchange data sensed by nodes (a descriptor of the collected data). In each node there is a resource monitor which monitors resources and modifies node behavior by changes. ADV, REQ and DATA are three SPIN messages for network data collection.

A Node broadcasts in the network, whether it has data to be sent, and ADV packets with data attributes. Interested nodes query for this node by sending a REQ request. This publicity node sends data to an interested node after receipt of REQ. ACQUIRE considers the network as a distributed database and similarly to complex queries is used to break into several small queries similar definition. ACQUIRE is here understood, and BS sends a query, which is sent, while each node is partially trying to address the query by using the pre-found information and then send it to the next node. ACQUIRE selects it randomly or according to the ability to satisfy a query, when selecting the next node.

3.4. Routing Protocol Based on Location

This facilitates re-missions or data to the predefined region using node position data to limit the data transfer degree. Subject to the location data of the node, there are definitely several routing protocols on the network that face the challenge. Nodes are normally separated from the instance of a node into shifted territories. The house-fixed data transmission will limit transmission run, decrease live contact between nodes and postpone the frame period. Data transmission can be limited.

Routing protocol based on location: the location-based routing protocol uses location data for management of routing disclosures, as well as for sending information. It also enables spatial data transfer and prevents data flooding in the system. Geographical Energy Aware Routing (GEAR:) This shows that each node retains its information of costs and a learning cost to reach the target across its neighbors. The projected cost typically consists of a combination of energy and distance. Most of the time, gaps arise when a node is not closer to the target.

If there are no vacancies, the measured costs are the same as the informed costs. This is a rebound when a packet completes its target in order to pursue a balanced path for the next batch. It is not only beneficial for GEAR to decrease the use of energy, but it also offers better packet transmission. GAF: GAF is being used for WSN because this supports energy efficiency. It is called geographic adaptive fidelity. GAF has three phases of discovery, transmit and sleep, for example [9]. If a sensor is in the sleep state, it shuts its radio for energy saving. A sensor exchange discovery messages which are used to discover various sensors in the network. In transmit state; a sensor periodically transmits its contact message to them to alarm similar sensors about its communication. GAF enlarges the lifespan of the node by saving energy.

3.5. QoS Based Routing Protocol

A lifespan aware QoS development is to be constrained to affirm the incredible use in the interim of all-out affiliation band calculation and rational imperativeness strategy; As a partner degree precedent, the QoS based routing protocol is compatible in line with military goals and crisis perception applications. MECN: To establish and maintain a base energy system for wireless networks via GPS, the Minimum Energy Communication Network (MECN). There are 2 phases for this Protocol: It takes 2D areas and creates a delicate graph that consists of a large number of restricted areas of each diagram node. The packet diagram includes the best energy usage relations. Considers the best links in the area map on the enveloped area. As a cost assessment, MECN uses the most suitable method of estimate with power utilization.

SMECN: a modification to MECN was also needed. Sensor finds his immediate neighbors in the SMECN protocol via a message of advertisement with a certain limited power which gradually refreshes. SMECN has a good benefit since it requires fewer resources than MECN, and the communication support costs are smaller.

4. OPEN RESEARCH ISSUES

In coming years, effective incorporation of cryptosystems with enhancements and routing protocols with optimized performance will try to meet requirements of energy efficient and secure routing protocols for various communication applications using WSNs. Reflecting algorithmic enhancements with newly available mathematical analytic models [24], with low complexity and lightweight processes, can play important role for security of nodes as well as

security of information which flow in the wireless sensor network. Also, improvements in authentication of nodes by discovering node's behavioral data is also an important mechanism which is used to detect, avoid and remove malicious nodes malfunctioning by intrusion like activities in the WSNs. Additionally, improved protocol for routing with better security parameters combined with better energy efficiency approaches promise best possible results for the secure and energy efficient systems and application using WSNs.

5. CONCLUSION

In this review of literature authors came to realization that in majority of existing systems have focused either on enhancing node or connection (link) authentication using cryptographic approaches, trust sensing techniques by analyzing behavioral data of nodes, or on enhancement of routing-based protocols. Some approaches are presenting enhancement in routing protocol with energy efficiency and others are providing solutions by diverse approaches for developing secure and energy efficient Wireless Sensor Networks [25]. Certainly, these given protocols and methods have performed a powerful role for nodes and data security, as well as tried to provide a better use of resources, such as computational power and battery. Though the efficiency and performance of all these approaches, especially for time, energy efficiency, processing power will be always a choice of future research and enhancement analysis. Additionally, over-heads in signaling, data transmission, control messages, required complexity in computation are required to further assessment to match future track of advanced applications, which will be more fast, energy efficient, deal in large data and QoS oriented. This literature review is aimed to make understanding of use of both security approaches of WSN nodes and information links and enhancements in routing protocols which will make potential better solutions. Security mechanisms, Still, with growing technical advancements and increasing demands of communication applications, computational complexity, processing delay, latency, memory usage, energy-consumption, throughput and reliability of WSNs will be open for further assessment, enhancements and research.

REFERENCES

[1] Carlos-Mancilla, M., López-Mellado, E., & Siller, M. (2016). Wireless Sensor Networks Formation: Approaches and Techniques. Journal of Sensors, 2016, 1–18. doi:10.1155/2016/2081902

[2] Ramasamy, V. (2017). Mobile Wireless Sensor Networks: An Overview. Wireless Sensor Networks - Insights and Innovations. doi:10.5772/intechopen.70592

[3] Kazem Sohraby Daniel Minoli Taieb Znati, Wireless sensor networks: technology, protocols, and applications, Wiley InterScience, Published by John Wiley & Sons, Inc., Hoboken, New Jersey, ISBN 978-0-471-74300-2

[4] N. Bandirmali and İ. Ertürk, "Increasing the reliability of security protocols for WSNs," 2009 International Conference on Application of Information and Communication Technologies,Baku, 2009, pp. 1-5, doi: 10.1109/ICAICT.2009.5372620.

[5] Xueqi Fan, Fransisca Susan, William Long, Shangyan Li, "Security Analysis of Zigbee" www.mit.edu, May, 2017

[6] Kardi, R. Zagrouba "Attacks classification and security mechanisms in Wireless Sensor Networks", Advances in Science, Technology and Engineering Systems Journal, vol. 4, no. 6, pp.229-243 (2019).

[7] N. A. Pantazis, S. A. Nikolidakis and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," IEEE, 2013.

[8] Wafa Akkari, Badia Bouhdid, Abdelfettah Belghith, LEATCH: Low Energy Adaptive Tier Clustering Hierarchy, doi: 10.1016/j.procs.2015.05.110 (ANT 2015)

[9] X. Huang, Y. Fang, Multiconstrained QoS multipath routing in wireless sensor networks, Journal of Wireless Networks 14 (4) 465-478 2008.

[10] Wei Wang, Hempel, M., Dongming Peng, Honggang Wang, Sharif, H., & Hsiao-Hwa Chen.(2010). On Energy Efficient Encryption for Video Streaming in Wireless Sensor Networks. IEEE Transactions on Multimedia, 12(5), 417–426. doi:10.1109/tmm. 2010.2050653

[11] Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2013). Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey. IEEE

Communications Surveys & Tutorials, 15(2), 551–591.doi:10.1109/surv.2012.062612.00084

[12] Aziz, A. A., Sekercioglu, Y. A., Fitzpatrick, P., & Ivanovich, M. (2013). A Survey on Distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor Networks. IEEE Communications Surveys & Tutorials, 15(1), 121–144. doi:10.1109/surv.2012 .031612.00124

[13] Zhao, M., Li, J., & Yang, Y. (2014). A Framework of Joint Mobile Energy Replenishment and Data Gathering in Wireless Rechargeable Sensor Networks. IEEE Transactions on Mobile Computing, 13(12), 2689–2705.doi:10.1109/tmc.2014.2307335

[14] Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 11(9),2013–2027.doi:10.1109/tifs.2016.2570740

[15] Tiloca, M., De Guglielmo, D., Dini, G., Anastasi, G., & Das, S. K. (2017). JAMMY: A Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs. IEEE Transactions on Dependable and Secure Computing, 14(4), 392–405. doi:10.1109/tdsc.2015.2467391

[16] Choi, J., Bang, J., Kim, L., Ahn, M., & Kwon, T. (2017). Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks. IEEE Systems Journal, 11(2), 494–502. doi:10.1109/jsyst.2015.2422736

[17] Gope, P., Lee, J., & Quek, T. Q. S. (2017). Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks. IEEE Sensors Journal, 17(2), 498– 503. doi:10.1109/jsen.2016.2628413

[18] Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., & Ding, Q. (2017). Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network. IEEE Access, 5, 9599–9609.doi:10.1109/access. 2017.2706973

[19] Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2017). SCOTRES: Secure Routing for IoT

and CPS. IEEE Internet of Things Journal, 4(6), 2129–2141.doi:10.1109/jiot.2017.2752801 [20] Alghamdi, T. A. (2018). Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method. IEEE Access, 1–1.doi:10.1109/access.2018.2865909

[21] Lee, Y., & Choi, J. (2018). Energy-efficient scheme using multiple antennas in secure distributed detection. IET Signal Processing, 12(5), 652–658. doi:10.1049/iet-spr.2017.0030

[22] Luo, X., Chen, Y., Li, M., Luo, Q., Xue, K., Liu, S., & Chenb, L. (2019). CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack. IEEE Access, 1–1.doi:10.1109/access.2019.2894637

[23] Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret Sharing-based Energy-aware and Multi-hop Routing Protocol for IoT based WSNs. IEEE Access,1–1. doi:10.1109/access.2019.2922971

[24] Devershi Pallavi Bhatt , Linesh Raja & Shilpa Sharma (2020) Light-weighted cryptographic algorithms for energy efficient applications, Journal of Discrete Mathematical Sciences and Cryptography, 23:2, 643-650, DOI: 10.1080/09720529.2020.1729510

[25] Bhatt, D. P., & Pareek, V. (2015). Lifetime Enhancement of Wireless Sensor Networks Using Fermat Point and Data Aggregation Mechanism. Emerging Research in Computing,