An Overview of Secure Routing Towards Wireless Sensor Networks

Naga Pavan Kumar Jammula
Lecturer, Depat of Information Technology,
College of Computing and Informatics, Wolkite University

Abstract- *Sensor nodes may constitute the network for observing physical marvels. Such network is called Wireless Sensor Network (WSN). Lion's share of WSN applications require in any event some level of security. Keeping in mind the end goal to accomplish the required level, secure and vigorous routing is vital. Secure information transmission is a basic issue for wireless sensor networks (WSNs). In a cluster-based WSN (CWSN), each cluster has a pioneer sensor node, viewed as cluster head (CH). A CH totals the information gathered by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the accumulation to the base station (BS). In this paper, we have reviewed different security issues and their countermeasure to lessen these issues.*

Keywords- Secure WSN, Energy Efficient WSN, Hierarchical routing, cluster head

I. INTRODUCTION

A. Wireless SensorNetwork

A sensor network is made out of tens to thousands of sensor nodes which are dispersed in a wide region. These nodes shape a network by speaking with each other either specifically or through different nodes as appeared in figure 1. At least one nodes among them will fill in as sink(s) that are equipped for speaking with the client either specifically or through the current wired networks.

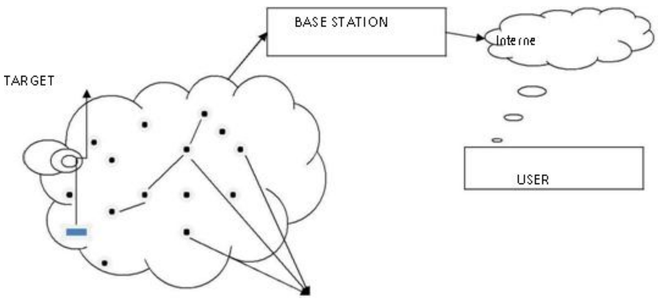

Fig. 1: Wireless Sensor Network architecture

B. Traffic patterns inWSNs

In contrast to customary networks, the WSNs show interesting awry movement designs. This is for the most part looked because of the capacity of the WSN which is to gather information, sensor nodes industriously send their information to the base station, while the base station just incidentally sends control messages to the sensor nodes. Also, the diverse applications can cause an extensive variety of movement designs. The activity of WSNs can be either singlehop or multi-jump. The multi-jump movement examples can be additionally separated, contingent upon the quantity of send and get nodes, or whether the network underpins in-network handling, into the accompanying (figure 2): Local Communication. It is utilized to communicate the status of a node to its neighbors. Likewise it is utilized to transmit the information between the two nodes specifically.

Point-to-Point Routing. It is utilized to send an information bundle from a self-assertive node to another subjective node. It is normally utilized as a part of a wireless LAN condition.

Meeting. The information parcels of different nodes are directed to a solitary base node. It is ordinarily utilized for information accumulation in WSNs. Accumulation. The information bundles can be handled in the transferring nodes and the total esteem is steered to the base node instead of the crude information.

Difference. It is utilized to send a summon from the base node to other sensor nodes. It is fascinating to explore the activity designs in WSNs alongside the versatility of the nodes, as node portability has been used in a couple of WSN applications, for example, medicinal services observing. One of the primary endeavors on doing this is given in [2]. In any case, there is as yet a progressing research territory that will accumulate awesome consideration on the next years.

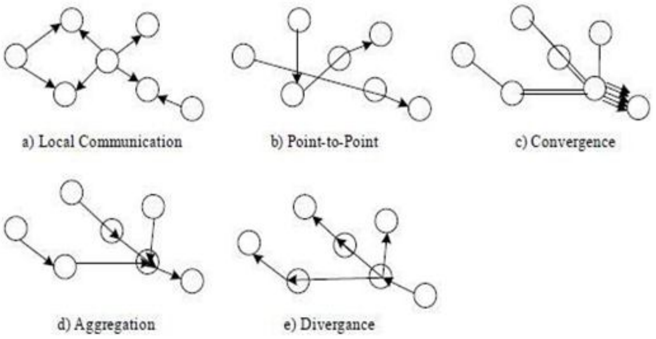

Fig. 2. The traffic patterns in WSNs

II. SECURITY ISSUES IN WIRELESS SENSORNETWORK

Despite the fact that, security worries in portable customary networks apply to sensor networks, the arrangements are not the same. Sensor nodes are firmly compelled as far as energy, preparing, and capacity limits. Once conveyed, it is frequently exceptionally hard to change or revive batteries for such nodes. This imperative restrains the quantity of traditional methods that can efficiently be embraced to sensor networks. Second, wireless correspondence makes data more powerless against assaults. Third, WSN need to scale to bigger quantities of elements than the present specially appointed networks. This requires watchful treatment of network estimate alterations, which can occur by outside assault as opposed to inner lack or redesign. An interloper may embed new outside nodes to the networks that sustains false information or keeps the entry of genuine information. Node may be incapacitated by physical harm. Forward, sensor nodes set into the physical situations; in this way it is frequently simple to trade off by an assailant. Moreover, it is easy to catch them physically and demolish them. Fifth, sensors networks made out of heterogeneous nodes with various abilities. Recognizing the conceivable dangers that may confront sensor networks will help in planning secure routing convention Table 1 compress the conceivable dangers that may confront routing convention in sensor networks [1,6].

A. Black HoleAttack

In Black Hole assault [8] the aggressor tries to gather the greater part of the information of the network and later drops it. In our reenactment we considered the case in which the gatecrasher has high introductory energy when contrasted with other ordinary nodes. In LEACH cluster heads are being chosen in view of the remaining energy of different nodes. Since aggressor is having higher starting energy so it ends up one of the cluster heads in the first round and even in later adjusts, as it isn't devouring any energy for information transmission. Subsequently it moves toward becoming cluster head in every one of the rounds. In the wake of getting to be cluster head it gets information from the majority of its cluster individuals, total it and later on don't forward the information to the base station.

B. Gray HoleAttack

In Gray Hole assault [8] at first, a noxious node abuses the LEACH convention to publicize itself as having a high likelihood to turn into a cluster head, with the expectation of capturing bundles, next, the node drops the blocked parcels with a specific likelihood. A Gray Hole may display its malevolent conduct in various ways. It basically drops bundles originating from certain particular node(s) in the network while sending every one of the parcels for different nodes. Another sort of Gray Hole assault is a node acts malevolently for some specific time length by dropping parcels yet may change to ordinary conduct later or it might bundles of certain bundle ID and forward alternate parcels. A Gray Hole may likewise show an arbitrary conduct additionally in which it drops a portion of the parcels haphazardly while sending different bundles, along these lines making its discovery considerably more troublesome.

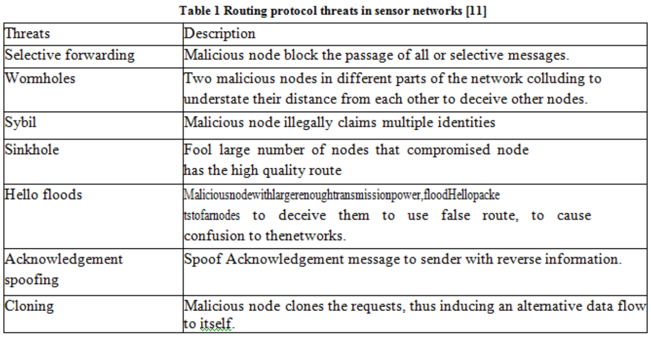

Table 1 Routing protocol threats in sensor networks [11]

Threats	Description
Selective forwarding	Malicious node block the passage of all or selective messages.
Wormholes	Two malicious nodes in different parts of the network colluding to understate their distance from each other to deceive other nodes.
Sybil	Malicious node illegally claims multiple identities
Sinkhole	Fool large number of nodes that compromised node has the high quality route
Hello floods	Maliciousnodewithlargerenoughtransmissionpower,floodHellopacketstofarnodes to deceive them to use false route, to cause confusion to thenetworks.
Acknowledgement spoofing	Spoof Acknowledgement message to sender with reverse information.
Cloning	Malicious node clones the requests, thus inducing an alternative data flow to itself.

III. SECURE AND ENERGY EFFICIENT ROUTING TECHNIQUES INWSN

In this paper [1], The creators propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by utilizing the identity-based digital signature (IBS) plot and the identity-based online/offline digital signature (IBOOS) conspire, separately. In SET-IBS, security depends on the hardness of the Diffie-Hellman issue in the blending area. SET-IBOOS additionally diminishes the computational overhead for protocol security, which is pivotal for WSNs, while its security depends on the hardness of the discrete logarithm issue. The creators demonstrate the possibility of the SET-IBS and SET-IBOOS protocols concerning the security prerequisites and security investigation against different assaults. In [2], energy efficient routing protocols are characterized into four fundamental plans: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols having a place with the principal classification can be additionally named level or hierarchical. The routing protocols having a place with the second classification can be additionally delegated Query-based or Coherent and non-reasonable based or Negotiation-based. The routing protocols having a place with the third classification can be additionally delegated Location-based or Mobile Agent-based. The routing protocols having a place with the fourth classification can be additionally named QoS-based or Multipath based. At that point, an expository review on energy efficient routing protocols for WSNs is given. In [3], an efficient key appropriation conspire is given which is valuable to secure data-driven routing protocols in Wireless Sensor Networks. Like these routing protocols, the proposed conspire bootstraps secure key conveyance with a concentrated procedure which gives a multi-level hierarchical association to WSNs. These two sorts of keys are helpful to secure individually data ask for dispersion and data sending through multi-jump routing ways. The creators in [4] proposed a streamlining model for network administration in multihop Wireless Sensor Networks (WSNs). Here, the creators build up an appropriated, twisted multipath calculation to convey the data from the data sources (focuses) to the Base stations (sinks) enabling the network to adjust to changes or disappointments. The Base Stations are strong nodes with abilities for situating themselves and conveying outside the network, which gifts them the advantage of knowing other Base Stations' situation in the territory of intrigue. Targets are nodes that produce data and need a settled measure of bandwidth to pass on this data to a Base Station. To build network's versatility, the gadgets inside the network will endeavor to make various ways from the earliest starting point attempting to reach no less than one Base Station. The model is understood through a heuristic calculation based on the closest neighbor and least bounce ideas. SIVA D. MURUGANATHAN et. al. [5] proposed a brought together routing protocol called Base-Station Controlled Dynamic Clustering Protocol (BCDCP), which appropriates the energy dissemination equitably among all sensor nodes to enhance network lifetime and normal energy reserve funds. Wireless sensor networks comprise of little battery controlled gadgets with constrained energy assets. In [6], the creator portrayed three new protocols for wireless sensor networks. One of these protocols, PEGASIS, is a voracious chain protocol that is close ideal for a data gathering issue in sensor networks. PEGASIS beats LEACH by wiping out the overhead of dynamic cluster arrangement, limiting the separation non-pioneer nodes must transmit, restricting the quantity of transmissions and gatherings among all nodes, and utilizing just a single transmission to the BS per round. Nodes alternate to transmit the intertwined data to the BS to adjust the energy consumption in the network and save the power of the sensor web as nodes kick the bucket at random areas. In [7], the creators have proposed LNT: a Logical Neighbor Tree for secure gathering administration that can be connected to a homogeneous WSN network with an asset obliged assemble controller. The plan reduces the gathering controller's errand by building a legitimate neighbor tree that conveys the rekeying messages. Execution examination has demonstrated that our plan beats some beforehand surely understood plans regarding calculation, correspondence and capacity costs. LNT plan can be enhanced by supplanting the ECC-based digital signature conspire by a more lightweight technique for validation, for example, the utilization of a key-chain. In [9], the creators have arranged a realistic energy show close by the trust based secure and energy-efficient clustering strategy for WSNs utilizing HBMA. The creators likewise contend that our energy show is the most apt for genuine situation, as it covers all the essential functionalities of a sensor node. For fitting the energy use among cluster heads, clusters closer to the base station are of littler sizes than remote ones from the base station. Subsequently cluster heads nearer to the base station protects some energy. For selecting a suitable cluster head the creators have likewise presented the most alluring TRUST component, which maintain a strategic distance from the pernicious node to be cluster head [9]. The creators in [10] have proposed an energy-efficient data gathering in wireless sensor networks (WSNs) that is based on a joining of the clustering and compressive detecting (CS). The creators presented the reconciliation of the CS with clustering to profit by the power sparing offered by the two strategies. The creators allude to our plan as clustered-base CS (CCS). The subsequent CS estimation matrices in CCS are as block diagonal matrices (BDMs). This paper [12] presents novel deterministic and half and half methodologies based on Combinatorial Design for choosing what number of and which keys to allocate to each key-chain before the sensor network arrangement. Secure interchanges in wireless sensor networks working under antagonistic conditions require giving pairwise (symmetric) keys to sensor nodes. For secure correspondence either two nodes have a key in like manner in their key-chains and they have a wireless connection between them, or there is a way, called key-way, among these two nodes where each combine of neighboring nodes on this way have a key in like manner. Length of the key-way is the key factor for proficiency of the plan. Specifically, Balanced Incomplete Block Designs (BIBD) and Generalized Quadrangles (GQ) are mapped to acquire efficient key circulation plans.

IV. CONCLUSION

A sensor network is made out of numerous sensor nodes which are sent in a wide region. These nodes frame a network by speaking with each other either specifically or through different nodes. At least one nodes among them will fill in as sink(s) that are fit for speaking with the client either straightforwardly or through the current wired networks. Wireless sensor networks can be used in a wide assortment of uses extending from war zone observation in military, through remote patient checking in solution to woods fire location in natural applications. Larger part of WSN applications require in any event some level of security. With a specific end goal to accomplish the required level, secure and vigorous routing is essential. Secure data transmission is a basic issue for wireless sensor networks (WSNs). The future work is to plan a routing protocol which is secure and solid. To secure the transmission, we can utilize encryption techniques and for unwavering quality we can utilize hierarchical routing or cluster based wireless sensor network. Clustering is a viable and down to earth approach to improve the framework execution of WSNs. Cluster-based data transmission in WSNs has been explored by analysts to accomplish the network adaptability and administration, which augments node lifetime and decrease bandwidth utilization by utilizing neighborhood coordinated effort among sensor nodes. In a cluster-based WSN (CWSN), each cluster has a pioneer sensor node, viewed as cluster head (CH). A CH totals the data gathered by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the total to the base station (BS).

REFERENCES

[1] Huang Lu, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND Conveyed SYSTEMS, VOL. 25, NO. 3, MARCH 2014 pp. 750-761.

[2] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey" IEEE COMMUNICATIONS SURVEYS and TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013 pp. 551-591.

[3] Abderrahmen Guermazi, "An Efficient Key Distribution Scheme to Secure Data-Centric Routing Protocols in Hierarchical Wireless Sensor Networks", The second International Conference on Ambient Systems, Networks and Technologies (ANT) Procedia Computer Science, 2011, pp 208– 215.

[4] Carlos Velasquez, " Multipath Routing Network Management Protocol for Resilient and Energy Efficient Wireless Sensor Networks", Information Technology and Quantitative Management, ITQM 2013 Procedia Computer Science 17, 2013, pp. 387 – 394.

[5] SIVA D. MURUGANATHAN, DANIEL C. F. Mama, ROLLY I. BHASIN, "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks", IEEE Radio Communications, March 2005.

[6] Stephanie Lindsey, Cauligi Raghavendra," Data Gathering Algorithms in Sensor Networks Using Energy Metrics", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 13, NO. 9, SEPTEMBER 2002.

[7] Omar Cheikhrouhoua, Anis, "LNT: a Logical Neighbor Tree for Secure Group Management in Wireless Sensor Networks", The second International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science 5, 2011 pp. 198– 207.

[8] Meenakshi Tripathi,M.S.Gaur,V.Laxmi, "Looking at the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", The eighth International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN) Procedia Computer Science 19, 2013.

[9] Rashmi Ranjan Sahoo, Moutushi Singh, Biswa Mohan Sahoo, "A Light Weight Trust Based Secure and Energy Efficient Clustering in Wireless Sensor Network: Honey Bee Mating Intelligence Approach", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), 2013.

[10] Minh Tuan Nguyen and Nazanin Rahnavard , "Cluster-Based Energy-Efficient Data Collection in Wireless Sensor Networks using Compressive Sensing", IEEE Military Communications Conference, 2013.

[11] Mostafa I. Abd-El-Barr Maryam M. Al-Otaibi Mohamed A. Youssef, "WIRELESS SENSOR NETWORKS-PART II: ROUTING PROTOCOLS AND SECURITY ISSUES", IEEE, May 2005.

[12] Seyit A. Camtepe, Bulent Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 2, APRIL 2007.

[13] Shoban Babu Sriramoju, "Heat Diffusion Based Search for Experts on World Wide Web" in “International Journal of Science and Research”, https://www.ijsr.net/archive/v6i11/v6i11.php, Volume 6, Issue 11, November 2017, 632 - 635, #ijsrnet

[14] Shoban Babu Sriramoju, “A Framework for Keyword Based Query and Response System for Web Based Expert Search” in “International Journal of Science and Research” Index Copernicus Value(2015):78.96 [ISSN : 2319-7064].

[15] Sriramoju Ajay Babu, Dr. S. Shoban Babu, “Improving Quality of Content Based Image Retrieval with Graph Based Ranking” in “International Journal of Research and

Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].

[16] Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].

[17] Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2014 [ISSN : 2249-4510]

[18] Mounica Doosetty, Keerthi Kodakandla, Ashok R, Shoban Babu Sriramoju, "Extensive Secure Cloud Storage System Supporting Privacy-Preserving Public Auditing" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2012 [ISSN : 2249-4510]

[19] Shoban Babu Sriramoju, "An Application for Annotating Web Search Results" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[20] Shoban Babu Sriramoju, "Multi View Point Measure for Achieving Highest Intra-Cluster Similarity" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[21] Shoban Babu Sriramoju, Madan Kumar Chandran, "UP-Growth Algorithms for Knowledge Discovery from Transactional Databases" in "International Journal of Advanced Research in Computer Science and Software Engineering", Vol 4, Issue 2, February 2014 [ISSN : 2277 128X]

[22] Monelli Ayyavaraiah, " A Study on Large-Scale Cross-Media Retrieval of Wikipedia Images towards Visual Query and Textual Expansion" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1238-1243 [ISSN : 2321-9653], www.ijraset.com

[23] Shoban Babu Sriramoju, Azmera Chandu Naik, N.Samba Siva Rao, "Predicting The Misusability Of Data From Malicious Insiders" in "International Journal of Computer Engineering and Applications" Vol V,Issue II,Febrauary 2014 [ISSN : 2321-3469]

[24] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Analysis on Image Compression Using Bit-Plane Separation Method" in "International Journal of Information Technology and Management", Vol VII, Issue X, November 2014 [ISSN : 2249-4510]

[25] Shoban Babu Sriramoju, "Mining Big Sources Using Efficient Data Mining Algorithms" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2, Issue 1,January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[26] Monelli Ayyavaraiah, "Nomenclature of Opinion Miningand Related Benchmarking Tools" in "International Journal of Scientific & Engineering Research" Vol 7,Issue 8, February 2018, [ISSN 2229-5518]

[27] Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198

[28] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays for Image Processing" in "International Journal of Information Technology and Management"
Vol V, Issue I, August 2013 [ISSN : 2249-4510]

[29] Dr. Shoban Babu Sriramoju, "A Review on Processing Big Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol-2, Issue-1, January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[30] Ajmera Rajesh, Siripuri Kiran, "Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com

[31] Shoban Babu Sriramoju, Dr. Atul Kumar, "An Analysis around the study of Distributed Data Mining Method in the Grid Environment : Technique, Algorithms and Services" in "Journal of Advances in Science and Technology" Vol-IV, Issue No-VII, November 2012 [ISSN : 2230-9659]

[32] Amitha Supriya. "Implementation of Image Processing System using Big Data in the Cloud Environment." International Journal for Scientific Research and Development 5.10 (2017): 211-217.

[33] SA Supriya. "A Survey Model of Big Data by Focusing on the Atmospheric Data Analysis." International Journal for Scientific Research and Development 5.10 (2017): 463-466.

[34] Shoban Babu Sriramoju, Dr. Atul Kumar, "An Analysis on Effective, Precise and Privacy Preserving Data Mining Association Rules with Partitioning on Distributed

Databases" in "International Journal of Information Technology and management" Vol-III, Issue-I, August 2012 [ISSN : 2249-4510]

[35] Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, [ISSN(ONLINE): 2395-1052]