International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 1 Issue 3, June 2015

Network Hole healing techniques for WSN

Shubhankan Sahu[1], Sapna Choudhary[2]
MTech Scholar CSE[1], Assistant Professor Department of Comp. Sc. & Engg.[2]
Shri Ram Group of Institution Jabalpur[1], Shri Ram Group of Institution Jabalpur[2]
shubhankan.sahu@gmail.com[1], choudharysapnajain@gmail.com[2]

Abstract: **The research on problems concerning holes in sensor networks is one of the major problems in WSN. Holes affect the network capacity and perceptual coverage of the network. In this paper we have categorized the hole on the basis of cause and effects. We have also presented pros and cons for the hole healing mechanism for wireless sensor network. Many techniques are proposed for hole detection. These mechanisms addresses a particular type of hole, here we have categorized them on the basis of type of hole they addressed.**

Index terms: WSN, Self healing, Voronoi, Jamming

I. INTRODUCTION

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. By networking large numbers of tiny sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways.

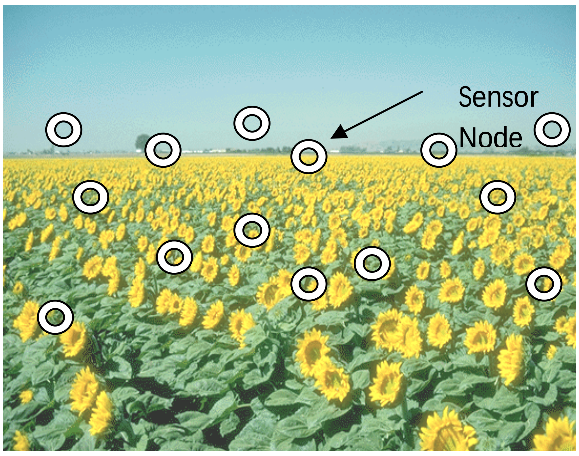

Figure 1: Wireless Sensor Network

In the coming years, as advances in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, increasing deployments of wireless sensor networks are expected, with the networks eventually growing to large numbers of nodes (e.g., thousands). Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring. therefore, the deployment is most often done by air plane dropping and this may often lead to unfair repartition of sensor nodes through the monitored region.

II. CHARACTERESTICS

The main characteristics and challenges of WSNs are:

A. *Cross-layer design*

Cross-layer is becoming an important studying in WSNs. the cross-layer can be used to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, QoS (Quality of Service), etc. Sensor nodes can be imagined as small computers which are extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors etc.

B. *Dynamic topology*

In many applications it is assumed that the topology of the network is stationary. However, in reality it is not, because WSN topology can change frequently. The topology of the WSNs can vary from a simple star net -work to a tree network or even to an advanced multi hop wireless mesh net -work.

C. Limited data rate and short distance

The sensor nodes electromagnetic range covers short distances (from one to several tens of meters). This determines the necessity of application multi-hop topology in WSN.

D. Different traffic intensity

The highest traffic density in WSN takes place around the central sensor nodes (that is the sink), because it collects all data coming from other nodes located in its vicinity. Quite the opposite, very little traffic takes place around sensor nodes which directly collect data and in the other direction, from sink to these nodes.

E. Energy constraints

The constraint most often associated with WSNs design is that sensor nodes operate with limited energy budgets. Typically, they are powered through batteries, which must be either replaced or recharged when depleted.

II. HOLE PROBLEM IN WSN

The research on problems concerning holes in sensor networks is one of the major problems in WSN. Holes affect the network capacity and perceptual coverage of the network. Due to limited battery the nodes may die with passage of time. In case of random deployment, there is a huge possibility that all areas of target region are not covered properly leading to formation of holes. Detection of holes is important because of their negative and damaging effects.

Qishi *et al.* [1] shown that the sensor deployment problem is NP-complete by reducing the Knapsack Problem (KP) [2] to a special case of the sensor deployment problem. Sensor deployment is a complex task in distributed sensor networks because of factors such as different sensor types and coverage ranges, sensor deployment and operational costs, and considerations for local and global coverage. Thus it is unlikely that polynomial time solutions that optimally solve the hole problem exist, which motivates us to consider approximate solutions.

TYPES OF HOLES AND THEIR COUNTER MEASURES

In this section we have reviewed various hole detection techniques on the basis of the type of hole problem addressed by them. Recently lots of hole detection techniques are proposed for WSN. These techniques are categorized by Perl *et al.* [3]as:(A) based on the type of information used, (B) based on computational model, and (C) based on network dynamics.

Nafaa Jabeur *et al.* [4] has presented four Curative Approaches for Sensor Network Holes, namely preventive, detective, repairing, and avoiding. Author also proposed different criteria for classification of holes on the basis of mobility, lifetime, purpose, affected function and cause.

There are four types of network holes [5] in wireless sensor network. We found that different types of hole posses different characteristics, for example hole may be created intestinally by intruders, or may be created due to node failure, or may be created due to routing problems. All the proposed hole detection mechanism addresses a particular type of hole, here we have categorized them on the basis of type of hole they addressed. In the following section reasons and detection measures are given for different types of holes.

A. Coverage hole

Coverage holes occurred if the target area is not fully covered with sufficient sensor nodes. No coverage hole exists if every point in the target area is covered by at least by required degree of coverage for a particular application.

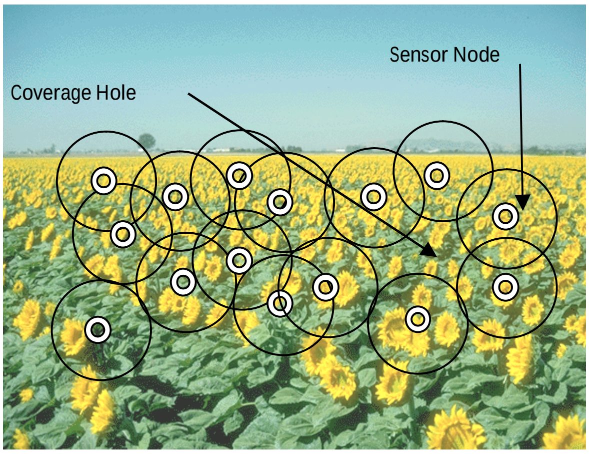

Figure 2: Coverage Hole Problem

These holes usually occur due to the random deployment of sensor nodes. In some cases, certain areas in the network are not covered with sufficient sensor nodes.

Detection Technique

X. Wang*et al.*[6] presents the design and analysis of a protocol that can dynamically configure a network to achieve guaranteed degrees of coverage and connectivity. Some theorems are proved and relationship between coverage and connectivity is analyzed. A Coverage Configuration Protocol (CCP) is presented that can provide different degrees of coverage requirement of the applications. This flexibility allows the network to self-configure for a wide range of applications and (possibly dynamic) environments.

W. Guilling *et al.* [7] have used Voronoi diagrams to discover the coverage holes and design three movement-assisted sensor deployment protocols, VEC(VECtor-based), VOR (VORonoi-based), and Minimax based on the principle of moving sensors from densely deployed areas to sparsely deployed areas. Proposed self-deployment protocols first discover the existence of coverage holes (the area not covered by any sensor) in the target area based on the sensing service required by the application. After discovering a coverage hole, the proposed protocols calculate the target positions of these sensors, where they should move.

X Li *et al.*[8] proposed a Triangular Mesh Self-organizing self-Healing protocol (3MeSH), to maintain sensing coverage over an entire wireless sensor network. It partitions the area into hexagonal cells, without requiring location awareness information. 3MeSH can conserve energy significantly by electing as few active nodes as possible, while accommodating a high tolerance to node positioning. This protocol used self-healing method. When active node failure occurs, the adjacent redundant nodes detect it, and elect new active nodes to cover the unsensed area i. e. hole.

Yao sun *et al.*[9] proposed an algorithm based on centroid calculation to locate the positions of the coverage holes. UAV is used to place the redeployment nodes. Considering UAVs characteristic, this paper assumes the route planning problem as the Traveling Salesman Problem (TSP), which can be solved by algorithms such as Genetic Algorithm (GA). Author has presented an easy way to detect and locate the coverage holes in WSN using graphical method. Since UAV has the maneuverability and the ability of moving straightly, the route planning problem is summarized as TSP to solve. From the experiment result, the algorithm presented in this work is proved feasible and efficient.

Chi-fu *et al.*[10] have formulated the coverage problem as a decision problem, whose goal is to determine whether every point in the service area of the sensor network is covered by at least k sensors, where k is a predefined value. The sensing ranges of sensors can be unit disks or non-unit disks. We present polynomial-time algorithms, in terms of the number of sensors that can be easily translated to distributed protocols. Author has proposed solutions to two versions of the coverage problem, namely k-UC and k-NC, in a wireless sensor network. Instead of determining the coverage of each location, this approach tries to look at how the perimeter of each sensor's sensing range is covered, thus leading to an efficient polynomial-time algorithm. As long as the perimeters of sensors are sufficiently covered, the whole area is sufficiently covered.

B. *Routing hole*

A routing hole consist of a region in the sensor network where either nodes are not available or the available nodes cannot participate in the actual routing of the data due to various possible reasons. These holes can be formed either due to voids in sensor deployment or because of failure of sensor nodes due to various reasons such as malfunctioning, battery depletion or an external event such as fire or structure collapse physically destroying the nodes.

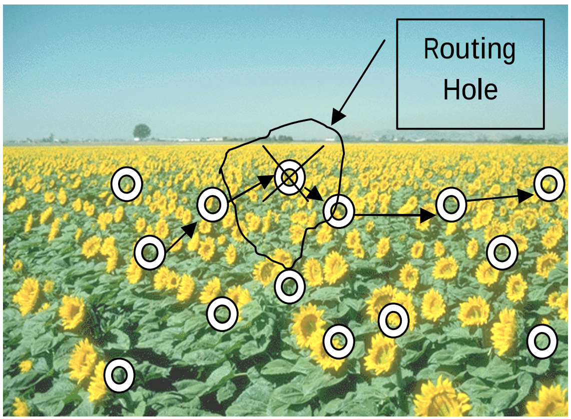

Figure 3: Routing hole

Detection Technique

Hsieh*et al.*[11] proposed a routing hole detection technique which obtains the boundary information of the holes and network. This boundary information can support the routing protocol such as GLIDER [12] to avoid the holes and increase the routing performance, or to promote the performance of sensor network applications or the implementation of networking functionalities.

The problem of discovering the nodes on the boundaries are investigated which may be inner that encircles the holes and outer that surrounds the network boundaries. Those selected boundary nodes are connected and could form the meaningful boundary cycles. Here, it is assume that each sensor node has a unique ID but without having location information, and its communication graph is a unit disk graph. In the network, the sensor nodes are randomly and densely deployed, and some irregular huge holes exist. All of nodes equally share the energy cost and only few nodes in the border area of holes and network need to pay much more energy to discover the boundary nodes. Accordingly, the network lifetime will be increased. This algorithm can precisely identify the boundary nodes even in sparsely deployed environment.

F. Qing *et al.*[13] used vornoi diagram and proposed simple and distributed algorithms, the Tent rule and Bound Hole, to identify and build routes around holes. In this work a mathematical definition of a communication void, i.e. a hole is given. Hole is defined to be simple regions enclosed by a (possibly concave) polygonal cycle which contains all the nodes where local minima can appear. It is shown that the local minimum phenomenon is simply caused by the existence of holes in the network. Routing in a network with all the holes identified beforehand can be very efficient.

In [14], by focusing on routing holes, the energy aspect of combating routing holes through the deployment of a single mobile(super) node is discussed. The specific contributions of the paper are:

It is proven that although bridging a routing hole by means of a mobile node may seems very intuitive, the deployment of the mobile is often hard to formally justify. For instance, the use of the mobile turns out to be completely energy unjustifiable in all circle and square like shaped holes, regardless of their actual size or number of boundary nodes actively involved in routing. Accordingly, the need to consider other parameters, such as overall transmission delay or static-node failure, when deciding whether/where to deploy the mobile, is demonstrated.

Building on above results, author proposed OPlaMoN– a simple distributed algorithm for determining the Optimal Placement of a Mobile Node within a routing hole of any arbitrary topology. As the name implies, the algorithm solves a rather complex optimization problem by breaking it into smaller fragments which are, then, partially solved by individual nodes. The final solution is reached through a cooperative decision-making process, assuming a minimum exchange of information among the effected nodes. The algorithm has excellent energy conserving properties and, as such, is highly suited for WSN environments.

Jianjung *et al.*[15] have proposed a heuristic hole detecting algorithm (HDAR) which can identify the hole in advance and advertise the hole information to those nodes that may be affected. HDAR focuses on defining and detecting holes in ad hoc network, representing holes and building routes around the holes. If the angle between two adjacent edges of a node is greater than 120 degrees, then it begins hole detection algorithm.

Here, the ratio of network distance over the Euclidean distance is used as metric to detect a hole. If for a node the value of hole detection ratio is greater than a predefined threshold, then it is on boundary. One of the main advantages is that a single node can efficiently detect the hole. After detecting hole, it advertises this information to nodes in vicinity which can adaptively adjust the forwarding direction. The contributions of this paper are threefold. First, it comes up with a heuristic algorithm to detect a hole quickly and easily. And the hole can be identified only by one time calculation. Second, it provides a concise representation of the hole. A hole is recorded as a segment. Third, development of an approach to let a subset of the nodes located on the hole's boundary announce the hole information to the nodes in the vicinity.

Shiawo *et al.*[16] designed an effective hole identification mechanism and proposed efficient hole bypassing routing scheme in wireless sensor networks with holes. With the proposed scheme, data packets are able to bypass holes and be delivered to the destination along a shorter path. Three major steps are used to avoid the routing holes.

1) *Construction of Hole Information:* In this step all the boundary nodes are informed about the existence of hole.
2) *Concave Region Identification:* In this step, concave regions of a hole are identified and thus data packets to be transmitted into these regions are avoided.
3) *Hole Bypassing Routing Scheme:* In this step alternate route is discovered to bypass the hole.

C. *Jamming hole*

A jamming hole [17] is another type of hole that can occur in tracking applications when the sensor node is tracked with jammers by jamming the radio frequency being used for communication among all the sensor nodes, here sensor node is able to find another sensor node in WSNs, but unable to communicate among them because of communication jamming.

Generally, jamming can be unintentional or deliberates. Unintentional jamming results if one or more sensor nodes continuously use the wireless channels to deny the communication facility among all the neighboring sensor nodes. In deliberate jamming, the opposition sensor node is trying to impair the communication among all the sensors nodes of the WSNs by interfering with the communication ability of the sensor nodes [18].

Fig. 4 depicts an example of jamming hole where jammer node radiates high radio frequency because of which all neighbor nodes cannot communicate with each other.

Here jamming hole is roughly similar to the routing hole. But routing hole is more dangerous than jamming hole, because, in jamming hole sensor nodes are alive, but in routing hole, sensor nodes are dead or act as dead.

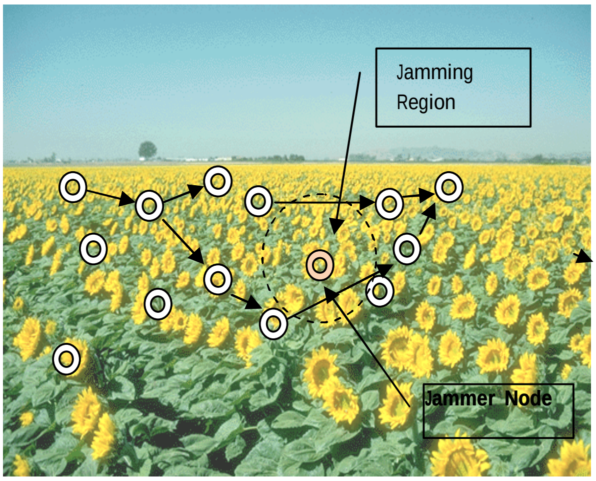

Figure 4 : Jamming Hole

Detection technique

Wood *et al.*[19] proposed JAM Protocol (Jammed-Area Mapping Service for Sensor Networks) mapping mechanism for jamming hole. Proposed mapping protocol uses loose group semantics integrated with eager eavesdropping to quickly build a map of a jammed region. Further variants and enhancements are presented in [20]. The JAM protocol works with almost all kind of jamming, independent of the layer were the attack takes place. When a node detects that it is jammed, it sends a JAMMED message to its neighbors, using some power management/carrier sense strategies to temporary override the jamming. Nodes which received jamming notifications group themselves, coalescing further to yield a map of the jammed region (also known as a jamming hole). However, this approach requires digital signal processing (DSP) capabilities and a library of patterns that may not be available except in military deployments. There is also a chance of network partitioning. This shortcoming can be compensated by the more powerful nodes used today.

Proanoet *al.*[21] have investigated the feasibility of real-time packet classification for launching selective jamming attacks. addressed the problem of selective jamming attacks and proposed three schemes for countering selective jamming in wireless networks. To mitigate selective jamming, cryptographic mechanisms such as commitment schemes [22], cryptographic puzzles [23], and all-in-one transformations [24], are combined with physical-layer parameters. The impact of various selective jamming strategies on the performance of the TCP protocol is presented. It is observed that for a TCP connection, a selective jamming attack TCP ACKs is significantly more harmful and efficient than all other jamming strategies.

Siddhabathula *et al.* [25] has proposed a collaborative detection scheme for fast jamming detection mechanism. The main idea is to evaluate the packet delivery ratio in an area instead of pairs of nodes since the attacker usually jams the area of his interest, not just the communication between some specific pairs of nodes. Time line is divided into multiple intervals and have sensor nodes periodically send out beacon signals. Loss of messages observed within each time interval for jamming detection. It is shown by experiment that there is a huge difference in the PDRs with and without jamming attacks. As a result, for a given time interval, if a node sees a significant drop on the number of beacons received from neighbors when compared to what was observed in the last time interval and it is assumed that this node is jammed. Certainly, frequently broadcasting beacon messages allows to detect jamming faster but consumes more energy and drains out the batteries of the nodes faster.

D. Sink/Black hole

A black hole [26] problem is caused by an external adversary on a subset of the sensor nodes in the network. The adversary captures these nodes and re-programs them so that they do not transmit any data packets, namely the packets they generate and the packets from other sensor nodes that they are supposed to forward. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it, is dramatically decreased.

Different locations of the attacker induce different influences on the network. If the attacker is located close to the base station, all the traffic going to the base station might need to go through the attacker. Obviously, black hole attacks in this case can break the communication between the base station and the rest of the WSN, and effectively prevent the WSN from serving its purposes. In contrast, if a black hole attacking node is at the edge of the WSN, probably very few sensors need it to communicate with others. Therefore, the harm can be very limited.

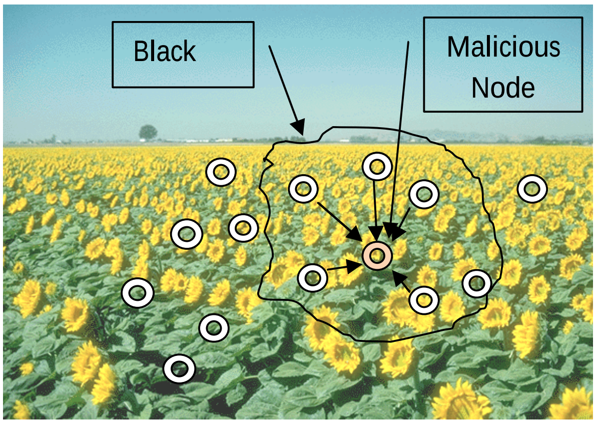

Figure 5: Black Hole

Detection Technique

The distributed strategy given in [27] uses the source node, the destination node and the neighbors of the intermediate nodes to detect and remove the malicious nodes. This solution divides the data packets into small sized blocks. By using this property, the malicious nodes can be detected between transmissions of consecutives small sized blocks. Then the source node sends a prelude message to the destination node to alert it about sending data. After ending the transmission, the destination node sends an acknowledgement via a postlude message to the source node containing the number of packets received by it. The source node checks this data and if it is not within the tolerable range, it sends a monitor message to all neighbors of the intermediate nodes on the route. The resulting messages coming from the monitoring nodes help the source node in judging whether the suspected nodes are malicious or not. However, this technique causes more delay in sending the total data.

In [28], Karakehayov proposed a technique in which transmitting sensor node performs power control to transmit a packet to more than one sensor nodes in the direction of the base station. If a sensor node that is on the forwarding path does not forward a packet, then its next hop neighbor on the forwarding path will identify this event and report the sensor node as a black hole. This scheme is very expensive – for a network with n black hole nodes, for each original message, O(n) extra messages are required, which is very expensive.

B.Yu [29] proposes a method to detect selective forwarding attacks based on checkpoints. Firstly choosing some nodes along the path randomly as the check points node, then after receiving data packets, there will generate corresponding acknowledgments and then transmit them to the upper way. If any checkpoints node doesn't get enough acknowledgments, it will generate Warning messages to the source node, so that the detection of the selective forwarding attacks can be realized. But an apparent problem exists in this process is that the nodes have to send acknowledgments continuously, which will greatly increase the cost of the network overhead. By the way, this method can't judge whether there malicious tamper action exists.

E. Worm hole

A worm hole is intentionally created by some adversary to attack the network. In the wormhole [30], [31] a malicious node tunnels messages received in one part of the network over a low latency link and replays them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. The tunnel can be established in many different ways, such as through an out-of band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. The tunnel creates the illusion that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops compared to the packets sent over normal routes. This allows an attacker to subvert the correct operation of the routing protocol, by controlling numerous routes in the network. Later, he can use this to perform traffic analysis or selectively drop data traffic.

Detection Technique

Yurong *et al.*[32] describes a distributed wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Since wormhole attacks are passive in nature, the algorithm uses a hop counting technique as a probe procedure, reconstructs local maps in each node, and then uses a "diameter" feature to detect abnormalities caused by wormholes.

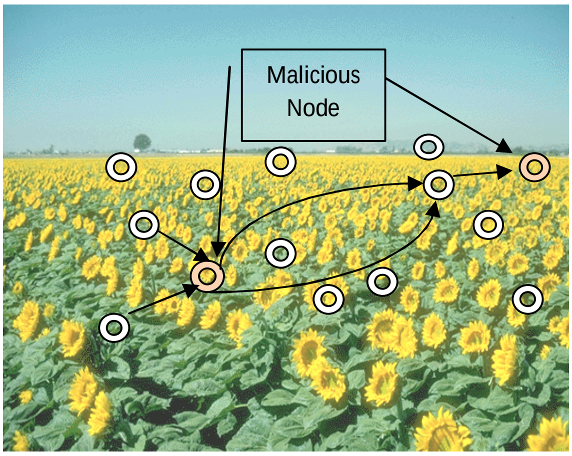

Figure 6 : Worm Hole

The main advantage of the algorithm is that it can provide the approximate location of wormholes, which is useful in implementing countermeasures.

Hu *etal.* [31] Proposed a solution for worm hole, called packet leashes, which is a general mechanism that can detect and prevent from a wormhole. A leash is a portion of information that is added to the packet to restrict its traveling distance or time. This solution consists of two types of leashes: geographic leashes and temporal leashes. A geographic leash detects and prevents the wormhole by ensuring that the sender and the receiver are within a specified distance. To do that each node must know its location and be timely synchronized with other nodes. When the sender starts sending the packets, it stores its location and the sending timestamp in the packet. Then, the receiver will calculate its location and the receiving timestamp and compare them with the values in the packet. By doing that, the receiver can detect if the sender is within its distance or not, which will help detection and prevention of the wormhole attack.

The other type of solution is a temporal leash. It detects and prevents the wormhole attack by ensuring that the packet's traveling time is within a specified period of time. To do that, all nodes must be timely synchronized in terms of their clocks. When the sender starts sending the packets, it stores its sending timestamp in the packet.

Then, the receiver can compare its receiving timestamp with the value in the packet. Therefore, the receiver will be able to detect if the packet traveled as fast as the specified transmission time.

Dong*et al.* [33] developed distributed detection methods by making as few restrictions and assumptions as possible. Author analyzed the wormhole problem using a topology methodology, and proposed an effective distributed approach, which relies solely on network connectivity information, without any requirements on special hardware devices or any rigorous assumptions on network properties. Author classified wormholes into different categories based on their impacts on topology and then designed a topological approach, which captures fundamental topology deviations and thus, locates the wormholes by tracing the sources leading to such exceptions. The detection algorithm is carried out in a distributed manner across the network to avoid dependence on a small portion of the network, which could become the target of the adversaries.

III. CONCLUSION

In this paper we have analyzed the hole problem in wireless sensor network. We have categorized holes in five categories. We have presented some measures for countering the problem. We find that different types of hole have different characteristic. All the solutions target a particular type of hole. It is required to devise a general hole detection and prevention mechanism which can handle all types of holes.

REFERENCES

[1]. Wu, Qishi, Nageswara SV Rao, Xiaojiang Du, S. Sitharama Iyengar, and Vijay K. Vaishnavi. "On efficient deployment of sensors on planar grid." Computer Communications 30, Vol. 14, 2007, pp. 2721-2734.

[2]. Chern, Maw-Sheng. "On the computational complexity of reliability redundancy allocation in a series system." Operations Research Letters 11, no. 5, 1992, pp. 309-315.

[3]. Pearl Antil and Amita Malik, “Hole Detection for Quantifying Connectivity in Wireless Sensor Networks: A Survey,” Journal of Computer Networks and Communications, 2014.

[4]. Jabeur, Nafaa, Nabil Sahli, and Ijaz Muhammad Khan. "Survey on Sensor Holes: A Cause-Effect-Solution Perspective." Procedia Computer Science 19 (2013), pp. 1074-1080.

[5]. Nadeem Ahmed , Salil S. Kanhere , Sanjay Jha, “The holes problem in wireless sensor networks: a survey”, ACM SIGMOBILE Mobile Computing and Communications Review, Vol 9, 2 April 2005.

[6]. X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, C. Gill, Integrated coverage and connectivity configuration in wireless sensor networks, in: Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA,2003.

[7]. W. Guiling, C. Guohong, and T. La Porta, "Movement assisted sensor deployment," in INFOCOM 2004. Twenty third Annual Joint Conference of the IEEE Computer and Communications Societies, 2004, Vol.4. pp. 2469-2479.

[8]. Li, Xiaoyun, and David K. Hunter. "3MeSH for full sensing coverage in a WSN without location awareness." In London Communications Symposium. 2005.

[9]. Sun, Yao, Chengdong Wu, Yunzhou Zhang, and Nan Hu. "Holes detection in wireless sensor network and redeploy route planning based on unmanned aerial vehicle." Journal of Information and Computational Science 9 (2012).

[10]. C. F. Huang and Y. C. Tseng, "The coverage problem in a wireless sensor network," Mobile Networks and Applications, 2005, Vol. 10, pp. 519-528.

[11]. Hsieh, Kun-Ying, and Jang-Ping Sheu. "Hole detection and boundary recognition in wireless sensor networks." In Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on, IEEE, 2009, pp. 72-76.

[12]. Q. Fang, J. Gao, L. J. Guibas, V. de Silva, and L. Zhang, “Glider: Gradient Landmark-based Distributed Routing for Sensor Networks,” in Proc. of INFOCOM, USA, March 2005, Vol. 1,.pp. 339-350.

[13]. F. Qing, G. Jie, and L. J. Guibas, "Locating and bypassing routing holes in sensor networks," in INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, 2004, Vol.4, pp. 2458-2468.

[14]. Vlajic, Natalija, and Nelson Moniz. "Self-healing wireless sensor networks: Results that may surprise." In Globecom Workshops, 2007 IEEE, pp. 1-6.

[15]. Yang, Jianjun, and Zongming Fei. "HDAR: Hole detection and adaptive geographic routing for ad hoc networks." In Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference IEEE, 2010, pp. 1-6.

[16]. Hwang, Shiow-Fen, Chia-Hsuan Yang, Yi-Yu Su, and Chyi-Ren Dow. "Energy efficient hole bypassing routing in wireless sensor networks." In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 4, pp. 576-580.

[17]. Proano and L. Lazos, "Selective Jamming Attacks in Wireless Networks", Proceedings of the 2010 IEEE International Conference on Communications 2010, pp. 1-6.

[18]. Damgård, Ivan. "Commitment schemes and zero-knowledge protocols." *Lectures on Data Security*. Springer Berlin Heidelberg, 1999, pp 63-86.

[19]. A.D. Wood, J.A. Stankovic, S.H. Son, JAM: A jamming-area mapping ser-vice for sensor networks, In: Proceedings of the 24-th IEEE Real-Time Systems Symposium (RTSS-2003), Cancun, Mexico, IEEE December (2003), pp. 286-297.

[20]. Wood, Anthony D., and John A. Stankovic. "Security of distributed, ubiquitous, and embedded computing platforms." Wiley Handbook of Science and Technology for Homeland Security (2006).

[21]. Proano, Alejandro, and Loukas Lazos. "Selective jamming attacks in wireless networks." In Communications (ICC), 2010 IEEE International Conference. IEEE, 2010. pp. 1-6

[22]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and counter measures", In 1st IEEE International Workshop SNPA'03, May 2003,pp. 293-315.

[23]. Juels and J. Brainard. Client puzzles, "A cryptographic countermeasure against connection depletion attacks" In Proceedings of the Network and Distributed System Security Symposium, 1999, pp. 151–165.

[24]. Rivest, Ronald L. "All-or-nothing encryption and the package transform." In Fast Software Encryption, Springer Berlin Heidelberg, 1997, pp. 210-218.

[25]. Siddhabathula, Kartik, Qi Dong, Donggang Liu, and Matthew Wright. "Fast jamming detection in sensor networks." In Communications (ICC), 2012 IEEE International Conference , pp. 934-938.

[26]. Xing, Kai, Shyaam Sundhar Rajamadam Srinivasan, Major Jose, Jiang Li, and Xiuzhen Cheng. "Attacks and countermeasures in sensor networks: a survey." In Network Security, Springer US, 2010, pp. 251-272.

[27]. Banerjee, S. "Detection / Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" 2008, pp. 0-5.

[28]. Karakehayov, Zdravko. "Using REWARD to detect team black-hole attacks in wireless sensor networks." Wksp. Real-World Wireless Sensor Networks (2005), pp. 20-21.

[29]. B YuB Xiao. "Detecting selective forwarding attacks in wireless sensor networks". In: Proce. of the 20th International Parallel and Distributed Processing Symposium, Rhodes Island, Greece, 2006, pp.1218-1230.

[30]. L. Hu and D. Evans. "Using Directional Antennas to Prevent Wormhole Attacks" In Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.

[31]. Y. Hu, A. Perring, and D.B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In Proceedings of 22nd Annual Conference of the IEEE Computer and Communication Societies, Vol.3, April 2003. pp.1976-1986.

[32]. Yurong Xu, Guanling Chen, James Ford and Fillia Makedon," Detecting Wormhole Attacks In Wireless Sensor Networks".

[33]. Dong, Dezun, Mo Li, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao. "Topological detection on wormholes in wireless ad hoc and sensor networks." IEEE/ACM Transactions on Networking (TON) Vol. 6, 2011, pp. 1787-1796.