.

Security Attacks in Wireless Sensor Networks

A Synopsis of the Ph.D. Thesis

Submitted to

Gujarat Technological University, Ahmedabad

by

Manish Patel
Enrollment No.:119997107007
Branch: Computer Engineering

Under the Supervision of

Dr. Akshai Aggarwal
EX-Vice Chancellor
Gujarat Technological University, Ahmedabad

Under the Co-Supervision of

Dr. Nirbhay Chaubey
Associate Professor
S.S.Agarwal Institute of Computer Science, Navsari, Gujarat, India

Under Doctoral Progress Committee

Dr. Haresh Bhatt
SAC, Indian Space Research Organization, Ahmedabad

Dr. Y. B. Acharya
Physical Research Laboratory, Ahmedabad

GUJARAT TECHNOLOGICAL UNIVERSITY

Abstract

Wireless sensor networks are differing from other ad hoc networks. In WSN nodes are resource limited. They are prone to failures. Their topology often changes. They are remotely managed. They are unattended after deployment. Adversary can capture nodes easily. Due to this fundamental characteristics security is very crucial for wireless sensor networks. Sensor nodes are vulnerable to many more attacks such as jamming, selective forwarding, Sybil, wormhole, sinkhole, jellyfish etc. Among all possible attacks wormhole is very dangerous because after launching wormhole an attacker can launch many more attacks. Launching the wormhole is very easy but detecting it is very hard. To launch the wormhole, an attacker does not need to know the secret material used in the network. Wormholes use low latency out of band channel that is not visible to other sensor nodes. By gathering the traffic it is possible to break security mechanism used in the network. Thus wormhole is a gateway to many more malicious attacks. We have presented wormhole detection mechanism for both static and mobility based wireless sensor networks and both the approaches have good detection accuracy. Also we have discussed variants of wormhole attacks and their impact in wireless sensor networks.

1 Brief Description on the State of the Art of the Research Topic

In this section, we have presented various existing methods for wormhole attack detection. Authors have presented geographical and temporal leash approach to detect wormhole attack [1,2]. Geographical leash approach requires that each node knows their locations. Temporal leash approach requires that each node to be equipped with tightly synchronized clock. Distance consistency approach is presented in [3] where the sensors measure the distances to their neighboring locators using the RSSI method. In [4], malicious nodes are detected when unreasonable rank values are found. In [5], challenge response delay measurement approach is presented in which clock synchronization or location information is not required. Timing based approach is presented in [6] where the assumption is when any node sent or received

a packet, it is able to record the time. Ranging based secure neighbor discovery approach in [7] is divided into three parts: ranging, neighbor table exchange and link verification. In range free anchor free localization approach diameter feature is used to detect the wormhole attack [8]. A pair wise key pre-distribution protocol is proposed in [9] to detect wormhole attack in which public and private keys are generated through one-way hash function. In [10] the authors have presented statistical analysis and time constraint based approach in which the sink node initiates statistical analysis and the link which is attractive in terms of traffic is defines as a suspicious link. Each suspicious link is validated through time constraints. In [11] authors have concluded that per hop high delay value indicates the presence of wormhole.

In [12], RTT based approach in multi rate adhoc networks is presented in which source node calculates the round trip time of all the neighboring nodes involved in the route including processing time, transmission time and propagation delay. Approach presented in [13] takes advantages of both watchdog and Delphi methods and has good detection accuracy. It does not require any additional hardware and high computational. In [14], RTT is used to generate neighbor information and then network is reconstructed by MDS. The limitation of this approach is detection of wormholes connected by short paths introduces some false positives. In [15], if the ACK message is not delivered to the previous node within the TTL limit, then it indicates the presence of wormhole. The ACK messages must be transmitted via different path than the original report is sent on and transmitted between nodes separated by two hops. Statistical analysis of multipath approach is presented in [16] in which based on the percentage of ACKs received, the destination will verify the presence of the wormhole attack. In [17], each node sends a packet will monitor its parent and if the parent node drops or tampers the packet, it indicates that parent node is connected by a tunnel. Each node is equipped with directional antenna for wormhole detection [18]. Hence, the neighbor relation is set only if the directions of both pairs match. A set of investigator nodes are distributed over the network in charge of monitoring the network topology [19]. All forms of wormhole attacks are detected because whole network is covered. Radio fingerprinting device is used in [20] for wormhole detection in which the signal features are extracted and they are used for device identification.

In [21], authors have presented node monitoring approach for wormhole detec-

tion. False positive occurs in case of hidden wormhole attacks. Local connectivity test is proposed in [22]. The malicious node report incorrect connectivity information. It does not require special hardware and synchronization. The communication cost for the test is low. If the size of the maximal independent set is equal or larger than forbidden parameter then it indicates the presence of wormhole [23]. NNT and ADT are proposed in [24]. The idea behind NNT (Neighbor Number Test) is that the number of neighbors of the malicious node is increased within its radius by creating fake links. The idea behind ADT (All Distance Test) is that due to the wormhole the path becomes shorter in the network. The wormhole is located by finding the fundamental topology deviations [25]. In the presence of wormhole attack, the network layout has distorted features otherwise the network topology should be flat [26]. MDS based detection using local topology does not requires any additional hardware and overhead is also low [27]. When both ends of two wormholes are very close, the approach fails to detect the attack. In [28], the authors have presented passive and real time wormhole detection in which if the attacker attracts less traffic then attack may not be detected. Due to the wormhole attack, the path length reduces significantly. Unit disk graph based approach is presented in [29] in which the two hop sub path is monitored by the nodes on a received route request. In [30], authors have presented visual-assisted wormhole attack detection in IoT-enabled WSNs in which nodes are unaware of their locations and they are allowed to move. The number of the correct decisions is getting higher as the network nodes are increased. Graph theoretic model is presented in [31] which requires a combination of cryptography and location information. It is based on symmetric cryptography and does not need time synchronization. It requires location aware guard nodes. Mobile beacon based detection approach is presented in [32] in which the mobile beacon moves in the networks to communicate with the static beacons. It has high detection probability and accuracy for localizing the attackers. In [33], location based keys is used for countermeasures against wormhole attack. It requires a group of mobile robots having GPS capabilities. Secure localization and key distribution based approach is presented in [34] in which two neighbor sensor nodes share communication key. It is practical, low cost and scalable for large scale WSN deployments.

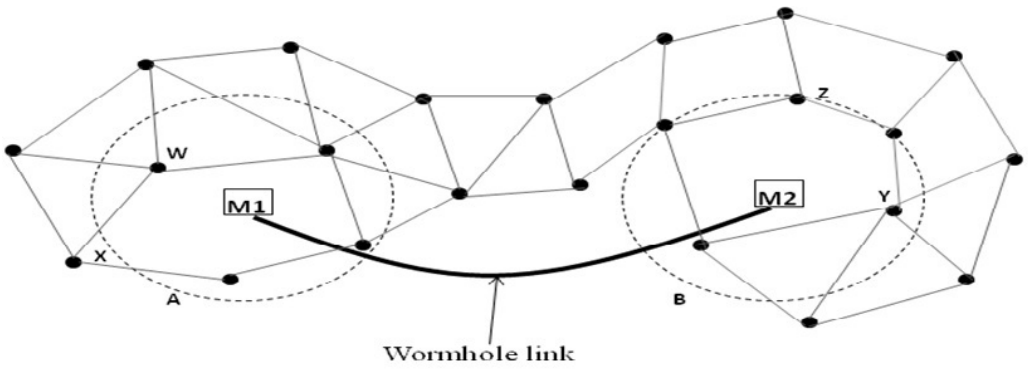

Figure 1: Wormhole tunnel constructed between nodes M1 and M2

2 Problem Definition

A wormhole attack involves a malicious node located in one area capturing packets and tunneling them to another malicious node located in another area of the network. Attackers can perform the wormhole attack without disclosing their identities.

As shown in Fig. 1, two malicious nodes M1 and M2 construct a tunnel. As a result, the nodes located in one part of the network believe that the nodes in the other part of the network are their neighbors and vice versa; thus, the entire routing process is disrupted. As a consequence, node Y believes that node W and node A are its one-hop neighbors. Similarly, node W believes that node Y and node Z are its one-hop neighbors. The attacker does not need any cryptographic break to launch the wormhole attack. Detecting this type of attack is very difficult because the attacker nodes use an out-of-band channel for tunneling packets. After succeeding in attracting traffic, the malicious node can launch many more attacks and can also drop packets, alter messages, and analyze the traffic. The nodes closest to the attackers would receive more packets and this would not only increase the responsibility of these nodes in terms of packet forwarding compared to other nodes, it would also waste their resources. This would cause an unfair workload distribution, resulting in inefficient resource utilization and a reduction in overall system performance.

3 Objectives and Scope of Work

Most of the methods employ hardware which increases the manufacturing cost of a sensor node. The existing work on wormhole attack detection has limitations in accuracy and applicability to wireless sensor networks. The existing algorithms are

resource hungry. Sensor nodes are resource limited devices. In a mobility based WSN, two genuine nodes becomes one hop neighbors which were many hops away from each other previously. It creates illusion that wormhole attack is present in the network. It is a challenging task to differentiate genuine nodes from the malicious nodes. Our goal is detection of the wormhole attack with high detection accuracy and low resource requirements.

4 Original Contribution

Our main contribution includes the following:

1. Survey of various security attacks and their countermeasures.
2. Identifying merits and demerits of existing techniques for wormhole detection.
3. Wormhole detection mechanism in static wireless sensor networks with low resource requirements and high detection accuracy.
4. Wormhole detection mechanism in mobility based wireless sensor networks with low resource requirements and high detection accuracy.
5. Variants of wormhole attack and their impact in wireless sensor networks.

5 Methodology, Results and Comparisons

5.1 Wormhole Attack Detection in Static WSNs

The sensor nodes after deployment are not movable. When sensor nodes are deployed, all nodes are legitimate nodes and no malicious nodes are present. For some initial interval, the network is safe and no attack has taken place and nodes have safely established their neighborhood information. One malicious node records packet from one area of the network and tunnel to the malicious node located in other area of the network.

Proposed protocol consists of three phases: (1) Build a neighbor list; (2) Neighbor list exchange and (3) Attack detection algorithm. At some point of time, node A overhears packets from some new nodes, say node B. Node B is a suspected node.

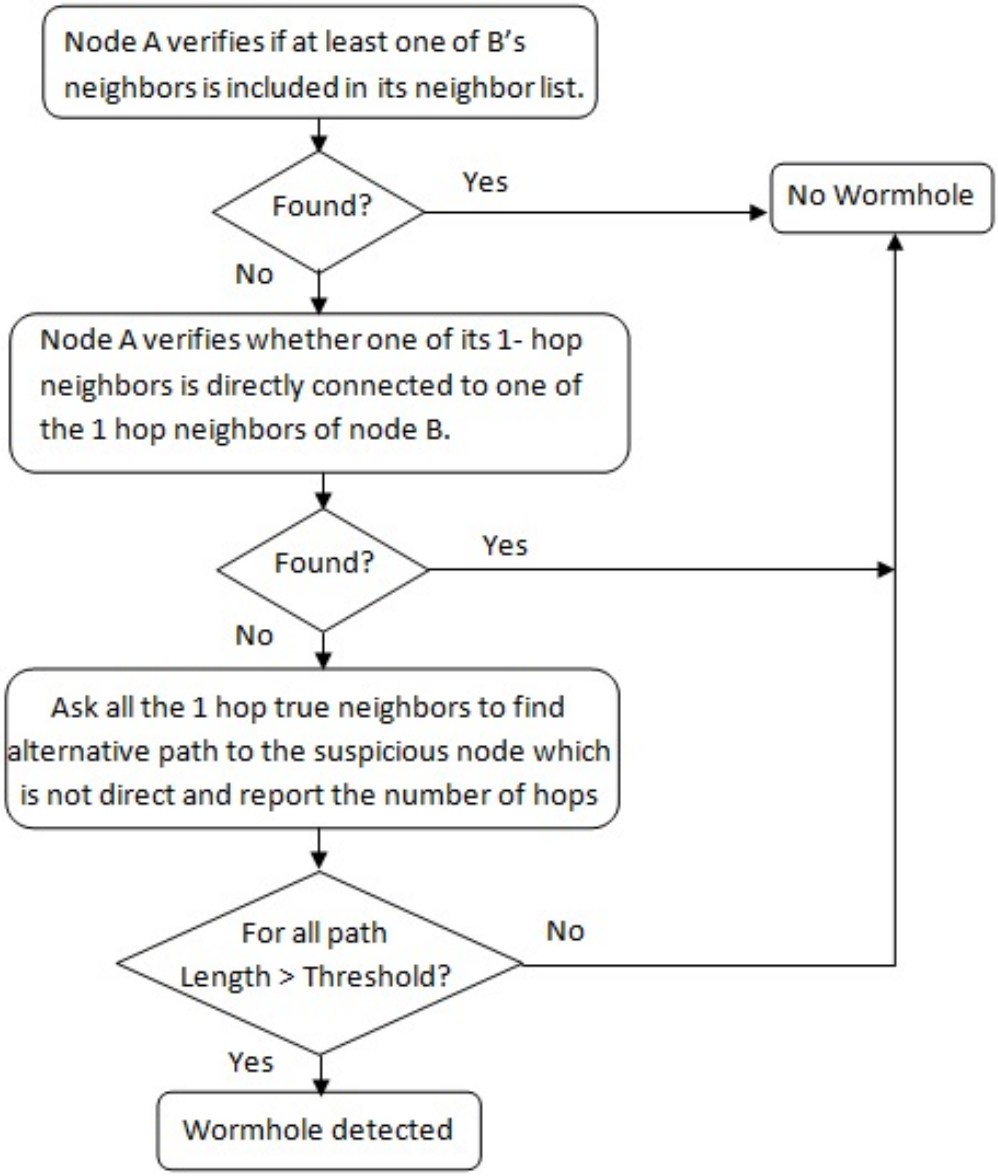

Figure 2: Wormhole Detection Methodology in Static WSNs

The neighbor list consists of two parts: trusted and suspected. Node B is added into suspected part. There might be a wormhole attack or not.

The average number of neighbors is represented by N_{AV}. The total number of nodes is represented by N_T. The size of ID is represented by S_{ID}. The storage cost required for storing the neighbor list is $S_{ID}N_{AV}$. The storage cost required to store the neighbors' neighbor list is $S_{ID}N_{AV}N_{AV}$. Total storage cost for each node is $S_{ID}N_{AV}+S_{ID}N_{AV}N_{AV}$. If S_{ID} is 4 bytes and N_{AV} is 10, then the storage cost is 440 bytes for each node. Wireless sensor node has flash memory of 512 kB and RAM of 4kB. Proposed protocol uses a small part of the memory and so it is suitable for resource constrained wireless sensor networks. Packet delivery ratio and throughput sharply decreases in the presence of an attack. After applying the proposed protocol

both packet delivery ratio and throughput have significant improvement. For reported path length, the threshold value λ taken is 3. Short wormholes are detected with $\lambda = 1$, but it will increase false positives. The false positives are reduced with $\lambda = 5$, but short wormholes are not detected. $\lambda = 3$ is the best suitable value to obtain good detection ratio. Pworm is a probabilistic method in which when little traffic is attracted then wormholes may not be detected [28]. In [14] few false positives occur with less no. of nodes and for short path wormhole. Accuracy analysis of the proposed method is shown in table 1.

Table 1: Accuracy Analysis

No. of Nodes	Pworm [28]	RTT Based MDA [14]	Proposed Approach
14	80	93	97
25	82	95	98
50	86	96	99
100	91	98	99

5.2 Wormhole Attack Detection in Mobility Based WSNs

The rate of change of the neighborhood (RCN) of any node A at time t is defined as,

$$RCN(t) = 1 - (N(t2) - P(t2, t1))/max(N(t2), N(t1))$$

where N(t2) is the no. of neighbor nodes of A at time t2, N(t1) is the no. of neighbor nodes of A at a previous time t1, and P(t2,t1) is the number of new neighbor nodes at time t2 in comparison to time t1. For example, node A announced that it had five neighboring nodes at time t1. In the next measurement, taken at time t2, it announces nine nodes and six of them were not present during the previous measurement at t1. So, $RCN(t) = 1-(9-6)/9$ = 0.66. If the value of RCN is greater than the predefined upper threshold then it indicates the presence of a wormhole attack. Conversely, if RCN is less than the predefined lower threshold then no wormhole attack is present in the network. If RCN lies in between the predefined lower and upper thresholds then all the new neighbors of A are added to the suspicious entry list. All the trusted neighbors of node A find the shortest indirect path to suspected node B and avoid the 1-hop neighbors of node A. Here the direct route from A to B is not included. The length of all paths is recorded. For all paths of which the length is greater than the

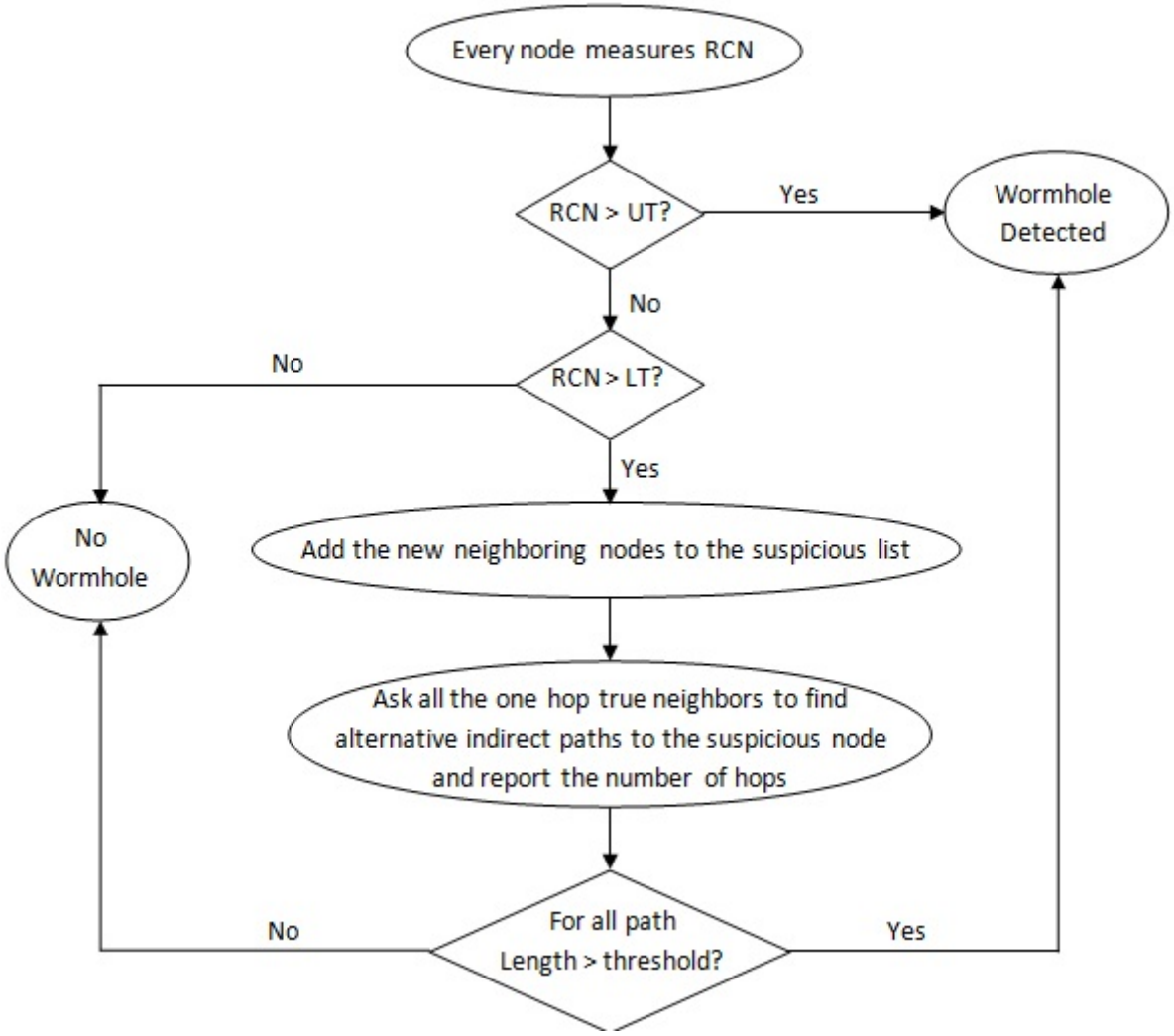

Figure 3: Wormhole Detection in Mobility Based WSNs

predefined threshold, the link $A \rightarrow B$ is declared a fake link and a wormhole attack is detected.

A node may possibly have very few neighbors, in which case the value of RCN would be high without the presence of a wormhole attack. If the time interval is longer, then the RCN value is higher for highly dynamic networks. Hence, the value of the time interval should be optimal. An optimal time interval value results in the value of RCN lying between 0.40 and 0.50. Using RCN = 0.46, we fixed the time interval for mobile nodes moving at different speeds. If the speed of the nodes increases, then the value of time interval should be decreased. The value of upper threshold (UT) is set to 1.50 * RCN. The value of lower threshold (LT) is set to 0.46. Detection Accuracy = $(TP + TN)/(TP + FP + TN + FN)$. For path length we have fixed the threshold value $\lambda = 3$. The simulation results show that the detection accuracy of our method is high in dense network. False positive increases when a

node may have very few neighbor nodes.

Table 2: Speed v/s Time Interval

Speed [m/s]	1	5	10
Time Interval [s]	52	27	11

Table 3: Accuracy Analysis

No. of Nodes	EyeSim [30]	WADP [21]	WRHT [13]	Proposed Approach
50	0.87	0.87	0.95	0.97
100	0.88	0.89	0.97	0.98
150	0.88	0.91	0.98	0.99
200	0.90	0.93	0.99	0.99

6 Variants of Wormhole Attacks in WSNs

6.1 Sinkhole Based Wormhole Attack

In sinkhole based wormhole attack the goal of an attacker is to attract the traffic and then selectively forward the packets. An attacker put one malicious node near to the destination node and another node near to the source. When the destination node sends route reply packet, it is captured by first malicious node and tunnels it to second malicious node. Source node and all its neighbors use path to the destination through second malicious node.

6.2 Denial of Service Based Wormhole Attack

When second malicious node receives route request packet from first malicious node, it broadcast to all its neighbors and the neighbor nodes send it to the destination. When the neighbor nodes receive the route request packet from the legitimate path, the packet will be dropped because it is a duplicate packet. The RREQ forwarded through the legitimate path cannot reach to the destination. When the destination node sends route reply packet, the neighbor nodes will not have reverse route to forward the RREP packets. The route reply packet is not forwarded by the neighbor nodes of the destination.

6.3 Blackhole Based Wormhole Attack

When the source node broadcast the RREQ packet, it is captured by malicious node and tunnel to another malicious node. Second malicious node replies it to the destination. When the destination node sends RREP packet, it is received by the source node via tunnel. In this way path is created between source and destination via malicious nodes. When the source node sends data packets, the packets will be dropped by the malicious node. It creates a black hole attack.

A RREP packet is captured by the malicious node M and it is tunneled to the target node T. The target node T forwards it to the source node. The source node and all other neighbor nodes mark the target node T as the first hop neighbor. The target node T has incomplete route towards the destination. Due to this all packets are dropped. It creates an indirect black hole attack.

6.4 Jellyfish Based Wormhole Attack

During the route discovery process, two malicious nodes establish tunnel and all the traffic reaches to the destination via this tunnel. Malicious node can launch jellyfish attack in three different ways: (1) Jellyfish attack by reordering the packets in which an attacker node reorders the data packets before the packets are forwarded. (2) Jellyfish periodic dropping attack in which an attacker selectively drops the packets. (3) Jellyfish delay variance attack in which an attacker delays packets randomly.

We have measured the impact of all these attacks in wireless sensor network. During the attack, packet delivery ratio and throughput decreases sharply.

7 Achievement

An approach presented in 5.1(Wormhole Attack Detection in Static WSNs) is suitable for resource constrained wireless sensor networks because it requires a small part of memory and it has good detection accuracy in comparison to other existing methods. In existing literature most of the wormhole detection approaches presented are for static WSNs because it is too difficult to get secure neighbor discovery in mobility based WSNs. Detecting wormhole attack in mobility based wireless sensor

networks is a challenging task. Our proposed method presented in 5.2 (Wormhole Attack Detection in Mobility Based WSNs) has good detection accuracy.

8 Conclusion

Security is very crucial for wireless sensor networks. Among all possible attacks, wormhole attack is very dangerous. Our proposed techniques have good detection accuracy and low resource requirements. Many solutions have been proposed but still it is an active research area. Future work includes analysis and detection of variants of wormhole attacks (Jellyfish, Denial of service, Black hole, Sinkhole etc.).

9 Publications

1. Manish M Patel et al; "Security Attacks in Wireless Sensor Networks: A Survey" IEEE International Conference on Intelligent System and Signal Processing, 1-2 March, 2013, Gujarat, INDIA. (IEEE)

2. Manish M Patel et al; "Two Phase Wormhole Attack Detection in Dynamic Wireless Sensor Networks" IEEE International Conference on Wireless Communications Signal Processing and Networking, 23-25 March, 2016, Chennai, INDIA. (IEEE)

3. Manish M Patel et al; "Wormhole Attack and Countermeasures in Wireless Sensor Networks: A Survey" International Journal of Engineering and Technology, Vol. 9, No 2, May-2017. (Scopus)

4. Manish M Patel et al; "Analysis of Wormhole Attack in Wireless Sensor Networks" 5th International Conference on Advanced Computing, Networking and Informatics, 01-03 June, 2017, NIT Goa. (Springer)

5. Manish M Patel et al; "Detection of Wormhole Attack in Static Wireless Sensor Networks" 2nd International Conference on Computer Communication and Computational Sciences, October 11-12, 2017, Phuket, Thailand. (Springer) (Best Paper Award)

6. Manish M Patel et al; "Performance Evaluation of Wireless Sensor Network in Presence of Wormhole Attack" 2nd International Conference on Advanced Computing and Intelligent Engineering, 23-25 November, 2017, Ajmer, India. (Springer)

7. Manish M Patel et al; "Variants of Wormhole Attacks and their Impact in Wireless Sensor Networks" International Conference on Computing Analytics and Networking, 15–16 December, 2017, Bhubaneswar, India. (Springer)

8. Manish M Patel et al; "Detecting Wormhole Attack in Mobility Based Wireless Sensor Networks" International Journal of Communication Networks and Distributed Systems. (Accepted) (INDERSCIENCE)

References

[1] Y. C. Hu, A. Perrig, and D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE Computer and Communications Societies, IEEE, vol. 3, pp. 1976–1986, 2003.

[2] Y. C. Hu, A. Perrig, and D. B. Johnson; "Wormhole attacks in wireless networks" IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, 2006.

[3] Honglong Chen,Wei Lou, Xice Sun and ZhiWang; "A Secure localization approach against wormhole attacks using distance consistency" EURASIP Journal on Wireless Communications and Networking, Volume 2010, 11 pages.

[4] Gu-Hsin Lai; "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network" EURASIP Journal on Wireless Communications and Networking 2016.

[5] S. Capkun, L. Buttyan and J.P. Hubaux; "SECTOR: Secure tracking of node encounters in multi-hop wireless networks" Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), pp. 21-32, Oct. 2003.

[6] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava; "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks"

IEEE Transactions on Wireless Communications, Vol. 8, and Issue: 2, 2009, pp. 736-745.

[7] Reza Shokri, Marcin Poturalski; "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks" ACM, WiSec'09, March 16-18, 2009, Zurich, Switzerland.

[8] Yurong Xu, Yi Ouyang, Zhengyi Le, James Ford, Fillia Makedon; "Analysis of Range-Free Anchor-Free Localization in a WSN under Wormhole Attack" ACM, MSWiM'07,October 22-26, 2007, Chaina, Greece.

[9] Mehdi Sookhak, Adnan Akhundzada, Alireza Sookhak, Mohammadreza Eslaminejad, Abdullah Gani, Muhammad Khurram Khan, Xiong Li, Xiaomin Wang; "Geographic Wormhole Detection in Wireless Sensor Networks" Journal of PLOS ONE, January 20, 2015, DOI: 10.1371/journal.pone.0115324.

[10] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao; "Detecting wormhole attacks in wireless sensor networks with statistical analysis" International Conference on Information Engineering(ICIE), 2010, pp. 251-254.

[11] Hon Sun Chiu, King Shan Lui; "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" 1st IEEE International Symposium on Wireless Pervasive Computing, 2006.

[12] Shams Qazi, Raad Raad, Yi Mu, Willy Susilo; "Securing DSR against wormhole attacks in multirate ad hoc networks" Journal of Network and Computer Applications, pp 582-593, 2013.

[13] Rupinder Singh, Jatinder Singh, and Ravinder Singh; "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks" Journal of Mobile Information Systems, Hindawi Publishing Corporation, Volume 2016, Article ID 8354930, 13 pages.

[14] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, Pragma Kar; "Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network" Journal of Computer Networks and Communications, Volume 2016, Article ID 3405264, 15 pages.

[15] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho; "A Secure routing method for detecting false reports and wormhole attacks in wireless sensor networks" Scientific Research on Wireless Sensor Network, March 2013, vol. 5, pp. 33-40.

[16] Lijun Qian, Ning Song, Xiangfang Li; "Detection of wormhole attacks in multipath routed wireless ad hoc networks: A statistical analysis approach" Journal of Network and Computer Applications, 2005.

[17] Sanjay Madria, Jian Yin; "SeRWA : A secure routing protocol against wormhole attacks in sensor networks" Journal of Ad Hoc Networks, September 2008.

[18] L. Hu and D. Evans; "Using directional antennas to prevent wormhole attacks" in Network and Distributed System Security Symposium (NDSS), pp. 131–141, 2004.

[19] Bayrem Triki, Slim Rekhis, and Noureddine Boudriga; "Digital investigation of wormhole attacks in wireless sensor networks" Eighth IEEE International Symposium on Network Computing and Applications, pp. 179-186, 2009.

[20] K.B. Rasmussen and S. Capkun; "Implications of radio fingerprinting on the security of sensor networks" Third International Conference on Security and Privacy in Communication Networks and the Workshops, pp. 331-340, Sep. 2007.

[21] J. Biswas, A. Gupta, and D. Singh; "WADP: a wormhole attack detection and prevention technique in MANET using modified AODV routing protocol" Proceedings of the 9th IEEE International Conference on Industrial and Information Systems (2014), pp. 1–6.

[22] Xiaomeng Ban, Rik Sarkar, Jie Gao; "Local Connectivity Tests to Identify Wormholes in Wireless Networks" ACM, MobiHoc'11, May 16-20, 2011, Paris, France.

[23] Ritesh Maheshwari, Jie Gao and Samir R Das; "Detecting wormhole attacks in wireless networks using connectivity information" IEEE INFOCOM, 2007.

[24] Levente Buttyan, Laszlo Dora, and Istvan Vajda; "Statistical wormhole detection in sensor networks" SAS 2005, Springer, pp. 128–141.

[25] Dong D, Liu Y, yang Li X, Liao X, Li M; "Topological detection on wormholes in wireless ad hoc and sensor networks" 17th IEEE International Conference on Network Protocols, 2009, pp. 314-323.

[26] W. Wang and B. Bhargava; "Visualization of wormholes in sensor networks" WiSe'04, Proceeding of the 2004 ACM workshop on Wireless Security, ACM Press, pp. 51-60, 2004.

[27] Xiaopei Lu, Dezun Dong and Xiangke Liao; "MDS-Based Wormhole Detection using Local Topology in Wireless Sensor networks" International Journal of Distributed Sensor networks, Volume 2012, Article ID 145702, 9 pages.

[28] Li Lu, Muhammad Jawad Hussain, Guoxing Luo, Zhigang Han; "Pworm: passive and Real-Time Wormhole Detection Scheme for WSNs" International Journal of Distributed Sensor networks, Volume 2015, Article ID 356382, 16 pages.

[29] Rakesh Matam, Somanath Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks" Springer, EURASIP Journal on Wireless Communications and Networking 2013.

[30] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, and A. Economides. "EyeSim : A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs" Proceedings of the 9th IFIP Wireless and Mobile Networking Conference (2016), pp. 103–109.

[31] Radha Poovendran, Loukas Lazos; "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks" Springer, Wireless Netw (2007) 13 : 27–59.

[32] Honglong Chen, Wendong Chen, Zhibo Wang, Yanjun Li, "Mobile Beacon Based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks" International Journal on Distributed Sensor Networks, Vol. 2014, 10 pages.

[33] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-Based Compromise – Tolerant Security Mechanisms for Wireless Sensor Networks" IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[34] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, “MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks” Elsevier, Journal of Ad Hoc Networks 6 (2008), 344-362.