# A Survey on Different Methods for Secure Measure against Wormhole Attack in Wireless Sensor Networks

P. Vijayalakshmi* & Dr.P.M. Gomathi**

*Assistant Professor, Department of Computer Science, P.K.R. Arts College for Women, Gobichettipalayam, Tamilnadu, INDIA.
E-Mail: vijiperumalsas{at}gmail{dot}com
**Head & Dean, Department of Computer Science, P.K.R. Arts College for Women (Autonomous), Gobichettipalayam, Tamilnadu, INDIA.

***Abstract*—**Wireless sensor networks (WSN) consists of a limited set of sensor devices that are regionally distributed in a particular indoor or external environment (generally predetermined). Generally, sensors are utilized for the environmental sensing and transfer the information to the base station. Wireless sensor networks are susceptible to attack or danger due to different kinds of extrinsic and internal attacks that are being restricted by computational resources, reduced memory capacity, low battery life, processing power & deficit of tamper resilient packaging. Security is emerging to be a primary challenge for these networks. This survey paper tries analyzing the threats posed on Wireless sensor networks and different routing attacks targeting the network layer. Especially, a highly dangerous attack is Wormhole attack and when the worm hole is set, adversarial nodes can exploit it to launch a Denial of Service attack, and it is an attack with the motive of shutting down a machine or network, so that it becomes unavailable to its respective users, where the attackers form a low-latency link between two points in the network. Highlighting the survey of previous techniques used for the detection of Wormhole attacks, researchers are endeavoring to find and distinguish the primary research concerns for Wormhole attacks detection in network layer.

***Keywords*—**Base Station; External and Internal Attacks; Malicious Nodes; Wormhole Attack and Denial of Service Attack.

***Abbreviations*—**Distributed Denial of Services Attack (DDoS); MAC Centralized Routing Protocol (MCRP); Maximum Likelihood Estimation (MLE); received signal strength indicator (RSSI); Trust and Energy Aware Secure Routing Protocol (TESRP); Trust Aware Distance Vector (T-AODV).

## I. INTRODUCTION

WIRELESS sensor networks, in the form of a segment of MANET includes a big number of small sensor nodes, which perform constant monitoring of the surrounding environment. Sensor nodes carry out different important tasks including signal processing, computation, and network self-configuration to extend the network coverage and improve its flexibility. The sensors combined exhibit a global condition of the environments, which provide more information compared to those rendered by individually functioning sensors. They are also accountable for environment sensing and transmission information. Generally, the transmission task is crucial due to the enormous amount of data and limited sensors devices. Since the sensor devices are less, the network is vulnerable to different kind of attacks [Govindasamy & Punniakody, 1; Sharma et al., 2].

Conventional security mechanisms are not suitable for WSNs since they are typically bulky and nodes are less in number. Moreover, these techniques do not defer the danger of other attacks. WSNs are helpful in different important domains like environment, industry, defence, healthcare, security and so on. For example, during a military operation, a wireless sensor network are required to monitor various activities. In case of the detection of an event, these sensor nodes perceive it and report the same to the base station (referred as sink) by interacting with other nodes [Singh et al., 3; Wu et al., 4].

Base stations are commonly utilized for gathering data from WSNs. They typically include enormous amount of resources (e.g. computational power and energy) compared to the usual sensor nodes that have approximately the same kind of limitations. Aggregation points collect the data from neighborhood sensor nodes, then combine them and relay them to base stations, where the data are processed further or relayed to a processing centre. In this manner, energy can be

preserved in WSNs and network life span is therefore extended. WSNs have few specific features making them different from other networks like MANET [Chen et al., 5].

The features, are listed as below, can make WSNs useful in practical scenarios: Sensor nodes has very less resources, like battery power, memory space and processing strength. Routing protocols and algorithms are desirable to make the sensor life last longer. WSNs are wireless networks that are capable of self configuration and self organization. The topology of sensor network various quickly and in ad-hoc. Sensor nodes are constantly included in and removed from the network. WSNs depict a centralized mechanism in terms of network management. The data flow from sensor nodes is directed towards some aggregation points which again relay the data to base stations. In addition, the base stations are capable of broadcasting query/control information to sensor nodes. Among the designs of WSNs, security is one of the primary features requiring immense focus, taking the prospective applications into consideration. Therefore, considering the security limitations into focus, this paper gives a short overview of the contemporary methods for wormhole attack detection in network layer. This way, the survey paper highlights on different techniques for the detection of wormhole attacks.

In this technical work, Section I provides the analysis of the importance of security model against wormhole attacks in wireless sensor network, Section 2 explains about the available security models in intended for wireless sensor network for wormhole attacks; Section 3 discusses the observations from the available works; Section 4 explains about the solution put forward for the problems faced in the available work; Section 5 provides the discussion of the simulation results. Section 6 discusses about the conclusion and work planned for the future.

## II. LITERATURE REVIEW

This section explains about the various techniques developed to achieve for security against wormhole attacks in wireless sensor network.

Ahutu & El-Ocla [6] introduced a compact multi-hop routing protocol for 802.15.4 WSN, whose aim is the reduction of the energy usage and also detection of the wormhole attacks. The results of simulation show that the MAC Centralized Routing Protocol (MCRP) performs better than other available contemporary protocols.

Patel et al., [7] suggested a wormhole detection approach that depends on neighborhood information and alternative path length calculation. The results of Simulation reveal that this technique improves detection accuracy with reduced storage demands.

Patel & Aggarwal [8] presented two phase detection approaches for wormhole attack in dynamic sensor networks. Security is a factor that arises from attacks. The wireless and distributive nature makes the network easy to be connected by anybody. Among all the probable attacks, wormholes are quite difficult to find since they can corrupt the network with no knowledge of the protocols utilized in the network. It is a strong attack, which can be carried without needs any cryptographic violations. It is very difficult to detect the wormhole attack. Results show that the proposed scheme yields reasonable detection accuracy.

Anwar et al., [9] demonstrated a trust aware distance vector routing protocol (T-AODV) to secure the wireless sensor network from wormhole attacks. It can be inferred from the experimental results that the network efficiency is much improved in terms of packet delivery ratio, end-to-end delay and number of node to the destination in the proposed scheme.

Kumar et al., [10] presented a localization algorithm, which averts the wormhole attack in mobile environment. The algorithm utilizes authentication process for finding any malicious nodes employing distance estimation method and uses Maximum Likelihood Estimation (MLE) to compute the right place. The comparison analysis of this algorithm and other existing algorithms shows the high efficiency of this algorithm.

Chen et al., [11] studied about a label-based DV-Hop secure localization approach to secure against the wormhole attack. It is also theoretically proven that the proposed approach is superior. The results of Simulation show the efficiency of the proposed label-based DV-Hop secure localization approach.

Shukla et al., [12] aimed for improved security achieved through Trust and energy aware secure routing protocol (TESRP) by protecting it against wormhole attack. TESRP is one of the effective trust based protocol, however this protocol does not ensure security from wormhole attack. In this work, trust algorithm along with sequence number concept has been utilized for protecting TESRP from wormhole attack.

Padmanabhan & Manickavasagam [13] introduced a flexible and distributed approach that makes use of sequential probability ratio tesdt, to prevent single point failures and to deal with high mobility, without needing extra resources. It is found that wormholes are identified with just a couple of packets and detection is quick with rising mobility. The system cannot customized easily since the system parameters can be selected for speed balancing and improve the accuracy of detection. System complexity in terms of communication, computation, and storage functions are evaluated and studied.

Sharma & Dwivedi [14] recommended a model for wormhole attack detection with the help of received signal strength indicator (RSSI) and this model aids in detecting the intruder node with high transmission strength.

Patidar & Dubey [15] studied about protocols that will secure the ad hoc networks from blackhole and wormhole attacks and help boost the stability of the network. This work introduced an intrusion detection system that relies on the principle of specification-based detection system for detecting and averting the blackhole attacks. This paper also introduces a hop count analysis mechanism for the detection of wormhole attacks along the paths in ad hoc networks. The proposed protocol does not need any location information,

time synchronization, or specialized hardware for wormhole attack detection. The evaluation of the protocols are carried out through testing and simulations carried out using network simulator.

Subha & Sankar [16] proposed a novel scheme which is known to be an effective wormhole detection approach in the wireless sensor networks. In this technique, the RTT between two sequential nodes and the neighbor number of those nodes is considered and this is required for the comparison between those values of other sequential nodes. The detection of wormhole attacks relies on two aspects. The first factor is that the transmission time between two wormhole attack infected nodes is much higher compared to that between two unaffected neighbor nodes. The second detection mechanism relies on the aspect that by bringing in new links into the network, the intruder forces to increase the number of neighbors pertaining to the nodes within its limit. The result of experiments reveals that the proposed approach yields improved network performance.

Luo et al., [17] defined CREDND, a protocol for launching a Credible Neighbor Discovery against wormholes in WSN, which can identify outside wormholes using the hop difference between the own specific neighbors and every intrinsic wormholes by facilitating the normal neighbor nodes to act as the witnesses for monitoring whether the authentication packets are relayed by intrusive nodes. CREDND is an easy, localized protocol and does not require specialized hardware, localization, or synchronization, but it enhances the strength of wormhole security. The results of simulation are studied, and it proves that CREDND performs better in wormhole detection compared to other similar solutions

Mandal & Sushil [18] studied about authentic wormhole attack tracking schemes. The significance of wormhole attack on packet transmission method and energy or resource balancing in a network is collected and correct recovery approaches are introduced to verify the solution for the DDoS (Distributed Denial of Services Attack) effect occurring because of wormhole attack.

Jagadeesan & Parthasarathy [19] suggested a novel model for the identification and elimination of blackhole and wormhole attacks in wireless ad-hoc networks. In order to perform this, a cross layer verification framework is introduced and its simulation is carried out in NS2 software to validate the efficiency. For the performance evaluation, the performance parameters measures are compared with those of the contemporary schemes. The proposed model can be recommended as a additional service support for cloud environment.

Ma et al., [20] recommended two types of defense mechanisms, which depend on monitoring neighbor node and node location information, to attain useful security against wormhole attacks employing packet encapsulation. The running state of the stable wireless sensor network is simulated under normal scenarios and during the launch of the wormhole attack employing OMNeT++ simulation platform. Also, the simulation of the network running process under wormhole attack is performed both by using the defense approach that depending on neighbor node monitoring and the defense mechanisms relying on node location information correspondingly. Through the evaluation of the particular defense effect, it is proven by the simulation results that the proposed defense mechanism is effective.

Table 1: Inferences from the Existing Works

| Author's name | Methods | Merits | Demerits |
|---|---|---|---|
| **Anwar et al., [9]** | Trust aware distance vector routing protocol | Improved packet delivery ratio | Very costly |
| **Chen et al., [11]** | label-based DV-Hop secure localization scheme | Increase in detection rate | Is not resilient to the packet loss |
| **Subha & Sankar [16]** | Innovative technique | Improved network performance | Reduced packet delivery ratio |
| **Patel & Aggarwal [18]** | Two phase detection techniques | Yields improved detection rate | Performance is not as expected in static network |
| **Kumar et al., [10]** | Localization algorithm | Reliable and adaptable | Increases the delay rate. |
| **Padmanabhan & Manickavasagam [13]** | scalable and distributed scheme | Reduces the overhead ratio | Very costly |
| **Ma et al., [20]** | Defense strategies | Yields good results | Decreases the throughput |
| **Luo et al., [17]** | Creating a Credible Neighbor Discovery | Performance is good | Reduced detection accuracy |
| **Sharma & Dwivedi [14]** | Received signal strength indicator | Increased detection rate | the error rate is increased |
| **Patel et al., [7]** | Neighborhood information and alternate path length calculation | Improved detection accuracy | Does not perform well in real time |
| **Ahutu & El-Ocla [6]** | Lightweight multi-hop routing protocol | Efficient and adaptable | Increased delay |

## III. INFERENCES FROM THE EXISTING WORKS

In the available works, Cross-Layer Medium Access Control, Ad-hoc On-demand Multipath Distance Vector routing protocol and duty-cycling operation models are used which rely on RTT for this attack detection. The round-trip time is defined as the time taken for the packet to be transmitted and for the acknowledgment to be got. The drawback for those techniques is that all the sensors in the network should possess a rightly synchronized clock, however it is a hard and costly task for the synchronized clocks to be implemented. And in few models, AODV enhancement is used, which acts as a protection against black hole and wormhole attacks. But, it shows only the hop count was utilized to decide if the node is legitimate or not. The drawback for these techniques is that it may ignore the authorized route, which is the shortest path to the destination.

## IV. SOLUTIONS

Wormhole attacks are only associated with network layer protocols. Since new routing protocols are introduced for WSNs, it is essential to analyze the probable disadvantages of these fresh routing protocols, the performance of these routing protocols with wormhole attack has to be analyzed and the efficiency of the available wormhole detection approaches on these protocols has to be examined. Therefore, a scope for further research surely exists in terms of performance analysis of the contemporary wormhole detection approaches on new routing protocols. The future work in this domain is aimed at more security improvements to be developed for routing protocols in wireless sensor networks. As research efforts further, an energy preserving secure measure relying on the network connectivity focused to identify the wormhole attack will be considered. The proposed metric is used on the ad-hoc on-demand distance vector routing protocol. The technique is only used by sensors of the chosen transmission path and their neighbors such that energy depletion and network complexity is optimized.

## V. RESULTS AND DISCUSSION

This section discus the experimental results of the secured AODV model which is implemented using NS2. Simulation parameter is shown in table.2.And to show the effectiveness of secured AODV model which is compared with the MCRP and TESRP models interns of packet delivery ratio, throughput, end to end delay and attack detection rate.

Table 2: Simulation Parameter

| Parameter | Value |
|---|---|
| **Network area** | 100m x 100m |
| **Network size** | 50,90,150 |
| **Sensors position** | random |
| **Transmission range** | 20 meters |
| **Transmission Range for wormhole nodes** | As long as the tunnel |
| **Mobility** | static |
| **Routing protocol** | AODV |
| **Simulation time** | 150 seconds |
| **Packet size** | 500 bytes |

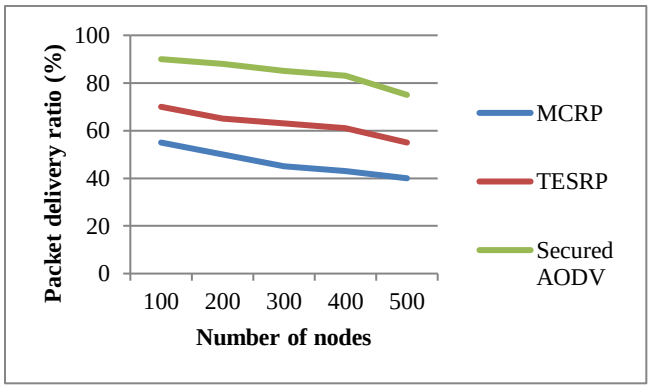


Figure 1: Packet Delivery Ratio Results vs. Classification Methods

Packet delivery ratio performance metric comparison between secured AODV, MCRP and TESRP are shown in figure.1. From the results it is concluded that secured AODV model produces the higher packet delivery ratio results of 81% while the MCRP and TESRP models produces only 40% and 55% accordingly.

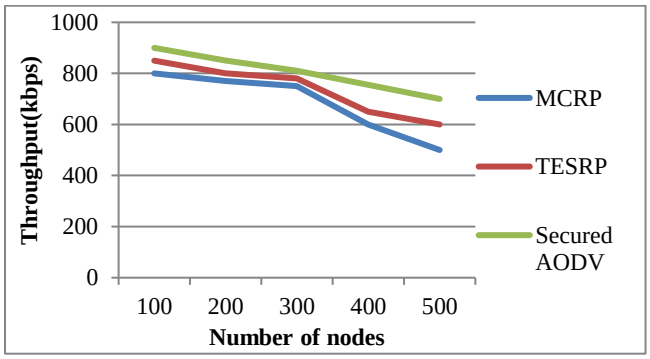


Figure 2: Throughput Results vs. Classification Methods

Figure 2 shows the comparison between secured AODV, MCRP and TESRP interms of throughput. From the results it is concluded that the secured AODV model produces the higher throughput results of 900(kbps) while the MCRP and TESRP models produces only 800(kbps) and 850(kbps) accordingly.

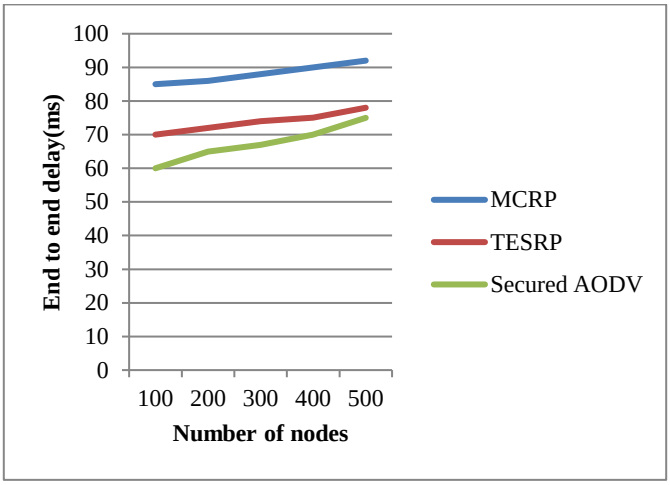


Figure 3: End to End Delay Results vs. Classification Methods

Figure 3 shows the comparison between secured AODV, MCRP and TESRP interms of End to End Delay. From the results it is concluded that the secured AODV model produces the lower End to End Delay results of 60(ms) while the MCRP and TESRP models produces 85(ms) and 70 (ms) accordingly.

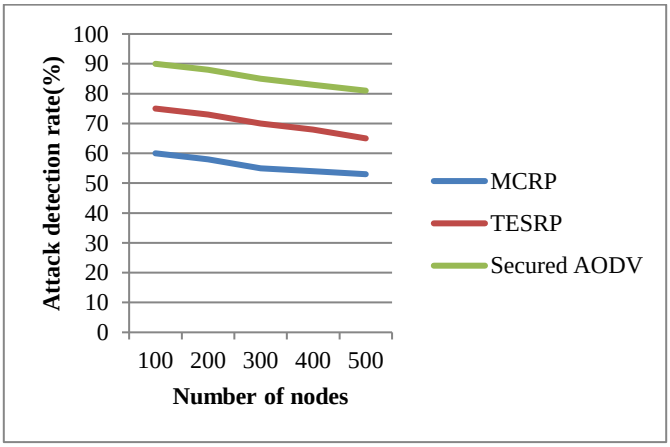


Figure 4: Attack Detection Rate vs. Classification Methods

Figure 4 shows the comparison between secured AODV, MCRP and TESRP interms of Attack detection rate. From the results it is concluded that the secured AODV model produces the higher Attack detection rate of 85(%) while the MCRP and TESRP models produces only 70(%) and 75(%) accordingly.

## VI. Conclusion and Future Work

Wireless sensor networks are susceptible to an extensive number of security attacks due to their implementation in a public and insecure environment. This survey paper investigated different available techniques to discover about their method of implementation for the wormhole attack detection. It has been found that among the number of mechanisms studied, every technique exhibits its own pros and cons and no real wormhole detection approach exists, capable of detecting all wormhole attacks fully. At last, by evaluating the strengths and weaknesses of the available approaches, the unresolved research problems in the wormhole detection area are analyzed. It is concluded that the future work in this field highlights on more security improvements for routing protocols in wireless sensor networks. As a part of future research, an energy preserving secure measure based on the network connectivity aimed at the detection the wormhole attack will be considered to be applied.

## References

[1] J. Govindasamy & S. Punniakody (2018), "A Comparative Study of Reactive, Proactive and Hybrid Routing Protocol in Wireless Sensor Network under Wormhole Attack". *Journal of Electrical Systems and Information Technology*, Vol. 5, No. 3, Pp. 735–744.

[2] M. Sharma, A. Tandon, S. Narayan & B. Bhushan (2017), "Classification and Analysis of Security Attacks in WSNs and IEEE 802.15. 4 Standards: A Survey", *3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), IEEE*, Pp. 1–5.

[3] M.M. Singh, N. Dutta, T.R. Singh & U. Nandi (2021), "A Technique to Detect Wormhole Attack in Wireless Sensor Network using Artificial Neural Network", *Evolutionary Computing and Mobile Sustainable Networks, Springer*, Pp. 297–307.

[4] J. Wu, H. Chen, W. Lou, Z. Wang & Z. Wang (2010), "Label-based DV-Hop Localization against Wormhole Attacks in Wireless Sensor Networks", *IEEE Fifth International Conference on Networking, Architecture, and Storage*, Pp. 79–88.

[5] H. Chen, W. Lou & Z. Wang (2009), "Conflicting-set-based Wormhole Attack Resistant Localization in Wireless Sensor Networks", *International Conference on Ubiquitous Intelligence and Computing, Springer*, Pp. 296–309.

[6] O.R. Ahutu & H. El-Ocla (2020), "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks", *IEEE Access*, Vol. 8, Pp. 63270–63282.

[7] M. Patel, A. Aggarwal & N. Chaubey (2019), "Detection of Wormhole Attack in Static Wireless Sensor Networks", *Advances in Computer Communication and Computational Sciences, Springer*, Pp. 463–471.

[8] M.M. Patel & A. Aggarwal (2016), "Two Phase Wormhole Detection Approach for Dynamic Wireless Sensor Networks", *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE*, Pp. 2109–2112.

[9] R.W. Anwar, M. Bakhtiari, A. Zainal, A.H. Abdullah & K.N. Qureshi (2015), "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks", *International Conference on Smart Sensors and Application (ICSSA), IEEE*, Pp. 56–59.

[10] G. Kumar, M.K. Rai & R. Saha (2017), "Securing Range Free Localization against Wormhole Attack using Distance Estimation and Maximum Likelihood Estimation in Wireless Sensor Networks", *Journal of Network and Computer Applications*, Vol. 99, Pp. 10–16.

[11] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang & A. Xia (2015), "Securing DV-Hop Localization against Wormhole Attacks in Wireless Sensor Networks", *Pervasive and Mobile Computing*, Vol. 16, Pp. 22–35.

[12] R. Shukla, R. Jain & P.D. Vyavahare (2017), "Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network", *International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, IEEE, Pp. 555–561.

[13] J. Padmanabhan & V. Manickavasagam (2017), "Scalable and Distributed Detection Analysis on Wormhole Links in Wireless Sensor Networks for Networked Systems", *IEEE Access*, Vol. 6, Pp. 1753–1763.

[14] P. Sharma & R.K. Dwivedi (2018), "Detection of High Transmission Power based Wormhole Attack using Received Signal Strength Indicator (RSSI)", *International Conference on Communication, Networks and Computing*, *Springer*, Pp. 142–152).

[15] K. Patidar & V. Dubey (2014), "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks", *Conference on IT in Business, Industry and Government (CSIBIG), IEEE*, Pp. 1–6.

[16] S. Subha, & U.G. Sankar (2015), "Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network", *IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, Pp. 1–4.

[17] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu & L. Chen (2019), "CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack", *IEEE Access*, Vol. 7, Pp. 18194–18205.

[18] S. Mandal & R. Sushil (2019), "Security Enhancement Approach in WSN to Recovering from Various Wormhole-based DDoS Attacks", *Innovations in Soft Computing and Information Technology*, *Springer*, Pp. 179–190.

[19] S. Jagadeesan & V. Parthasarathy (2019), "Design and Implement a Cross Layer Verification Framework (CLVF) for Detecting and Preventing Blackhole and Wormhole Attack in Wireless Ad-Hoc Networks for Cloud Environment", *Cluster Computing*, Vol. 22, No. 1, Pp. 299–310.

[20] R. Ma, S. Chen, K. Ma, C. Hu & X. Wang (2017), "Defenses against Wormhole Attacks in Wireless Sensor Networks", *International Conference on Network and System Security*, Pp. 413–426.