International Journal of Control and Automation
Vol.10, No.7 (2017), pp.89-96
http://dx.doi.org/10.14257/ijca.2017.10.7.08

Design of Distributed Approach for Wormhole Attack Detection in Wireless Sensor Networks

Manpreet Kaur[1], Gulshan Kumar[1*], Mritunjay Kumar Rai[1], Rahul Saha[1] and Hye-jin Kim[2]

[1]Lovely Professional University, Punjab, India
2Business Administration Research Institute, Sungshin W. University, Seoul, Republic of Korea
mvirdi93@gmail.com, gulshan3971@gmail.com, raimritunjay@gmail.com, rsahaaot@gmail.com, hyejinaa@daum.net

Abstract

In this paper we propose a distributed scheme to provide security against wormhole attack in Wireless Sensor Networks (WSNs). Some existing approaches are based on the detection and prevention schemes and other for correction of wormhole attack. In our study, we propose the scheme for distributed detection of wormhole in wireless sensor networks. Cryptographic mechanism of public key cryptosystems is used to maintain the integrity, authenticity, confidentiality and non-repudiation of message transmission. The wormhole detection methodology consists of three phases: initialization phase, neighborhood discovery with only one hop neighbors and wormhole detection process. The proposed scheme can help to find the wormhole attack in given network, if exists. The scheme does not even use any special hardware like directional antennas, or highly synchronized clocks.

Keywords: *Wireless Sensor Networks, Wormhole attack, Cryptographic Mechanisms, Public-key Cryptosystem, Zone Routing Protocol.*

1. Introduction

In today's technology era, we have immense power of technological advances which enable today's man to perform good for society and contribute to mankind by developing new technologies and researches in this huge world. The term Wireless Sensor Networks [1] can be defined as: "A wireless network with no fixed infrastructure that consists of sensor nodes which communicate with each other in the network via wireless transceivers." A wireless sensor network consists of three major components[2]: Sensing node is any normal sensor node that collects data from surrounded environment and transmit to nearby sink node. Sink node is like 'sensor head' which receives the collected data from sensor nodes and performs the local calculations over sensed information sent from sensing nodes. For multiple sensing nodes, there is one sink node. Wireless transceivers help sensor nodes to communicate with each other within the network. The deployment of sensor network can be affected by various constraints[3]: memory requirements, energy requirements, computational speed and communication bandwidth required, etc. Application areas for WSNs are[4]: military services, surveillance setup, commercial sector, medical field, battlefield, logistics and manufacturing, home automation, etc. There are numerous of attack possible to launch in wireless sensor networks[5]: blackhole attack, grayhole attack, sybil attack, sinkhole attack, byzantine attack, DDoS attack, vampire attack, wormhole attack, etc. The major challenges faced by WSNs are[6]: Spectrum allocation, Media access, Routing techniques, Multicasting, Energy efficiency, TCP performance, Service location, Security of information, etc.

Copyright ⓒ 2017 SERSC

The wormhole attack can be defined as[7], “the scenario in network when an intruder/s create tunnel/s at distinct ends in network and bypass the communication channel of other valid nodes by providing them false neighborhood information and receiving most of the network traffic and discarding it.” The malicious nodes in the network are called as wormhole nodes and the tunnel they created is called as wormhole link. Worm Hole attacks can be of two types: Hidden wormhole and Exposed / byzantine wormhole. There are various countermeasures to deal with WH attack each with their different advantages and disadvantages[8]: time-based solutions, location-based solutions, end-to-end based solutions, hop-count analysis based solutions and statistics based solutions.

The clustering can be defined as[9]: **“**The process of classifying group of nodes and group them on the basis of their characterization or attributes**”**. The clustering shows the distributed nature of deployed network. In clustering we are having two important nodes: cluster head and member nodes. The cluster head are the only form of communication with another cluster’s nodes. Member nodes are the other nodes present in the cluster and is monitored by the cluster head. There are two types of communication possible in clustering: Inter-cluster communication and Intra-cluster communication.

The zone routing protocol is a hybrid protocol for routing in clustered networks[10]. It is hybrid because it use good features from both proactive and reactive protocols. In ZRP, we are having the nodes clustered into different zones based on some distance or range. In ZRP we have two nodes: peripheral node and interior node. In ZRP, we are having two types of routing algorithms[11]: Inter-zone routing protocol and Intra-zone routing protocol.

2. Literature Review

In literature review, different techniques in order to mitigate the problem are found. But they are not enough for the growing need of security for the networks. Today’s time requires a distributed approach. In study of [12]work proposed for fault tolerance using spider-net ZRP in the mobile sinks of WSNs proposed by Shih Hao Chang and Ping Tsai Chung, aim is to propose a scheme for energy-efficiency, reliability and improved performance in WSNs mobile sinks. In [13] key management methodology for securing transport and network layers in MANETs using ZRP and WTLS key management is proposed, aim is to providing security to layers authentication, communication privacy and integrity of data and to defend against DoS attack.

In study of [14] a scheme for detection as well as prevention of wormhole attack exists in WSNs using AOMDV routing protocol which is proposed by Parmar Amish and V.B. Vaghela, aims to detect and prevent wormhole attack in WSN using AOMDV protocol.

In study of [15] an approach for design and implementation of trust based approach in order to reduce the various attacks occurring in MANETs presented by Nilesh N. Dangare and M.S. Mangrulkar, the aim is to mitigate Vampire and DDoS attacks. The author’s in [16] presented wormholes virtualization concept in WSNs is presented, the aim of the work is to propose such a mechanism that can detect wormholes in sensor network.

In study of [17] a mechanism for defense against wormhole and DoS attack in WMNs, the proposed technique finds wormhole free routes in networks by some finite state model and priority mechanism. A mechanism to create a secure neighborhood [18] in wireless ad hoc networks with the help of discrepancies in hop count is proposed which aims to create secure neighborhood by using hop count discrepancies in routing to detect true neighbors and remove those links that appear to be neighbor but in real are not. In the proposed work by authors, source node will discover its one-hop neighbor. A localized scheme for detection and prevention of wormhole in wireless networks presented [19] the proposed scheme has a capability to defend against wormhole attacks in wireless networks by not adopting any specialized hardware.

In study of [20] identifying wormholes on the basis of local connectivity tests in wireless networks is proposed that detect and remove wormhole using LCTs. A detailed case study on mobile adhoc networks protocols for routing [21] to check their performance over transmission control protocol and hypertext transfer protocol is presented the aim is to find out efficient routing protocol for routing among DSR, OLSR and AODV. Author's in [22] presented a novel secure method for node localization using concept of insider node validation and mutual authentication to mitigate several attacks noticed in localization in WSNs.

3. Proposed Work

In our proposed research work, a distributed approach is used. We make use of cryptography concepts of public and private cryptosystems. The concepts of clustering is also used by making base station as a most privileged nodes than other privileged and sensor node, which provide the communication between inter-cluster base stations in order to route the communication of simple sensor nodes and privileged nodes. The algorithm starts with initialization phase followed by neighborhood discovery only with one hop neighbors and then the wormhole detection process is executed. The following assumptions are made for the proposed algorithm:

- Base Station (BS) is secure enough and also works as Certification Authority (CA).
- BS provides certificates and required keys (public or private) to all the sensor nodes and privileged nodes.
- Nodes are pre-deployed with keys and are known to BS.

The proposed algorithm consists of three phases as follows:

- **Phase I: Initialization**

  All the nodes are pre-installed with public keys of base station. Base station distributes the certificates to all the nodes, both privileged nodes and sensor nodes, as follows:

$$BS \rightarrow u_i :\ \ Cert_{u_i} = [ID_{u_i}, t_{exp}^{u_i}]K +_{BS}$$
$$BS \rightarrow a_j :\ \ Cert_{a_j} = [ID_{a_j}, t_{exp}^{a_j}]K +_{BS}$$

  The u_i is for the sensor nodes and a_{id} is for privileged node.

- **Phase II: Neighborhood establishment**

  The privileged nodes broadcast a HELLO message to start the process of neighborhood discovery. The message is comprised of the following components:

$$HELLO: \{ ID_{a_j}, [t_{exp}, nonce]_{K+_{u_i}} \}$$

  Where, a_{id} is the ID of the privileged node, t_{exp} is the expiry time of the HELLO message, *[nonce]* is a random number encrypted with sensor node's public key.
  Upon receiving the HELLO message, the one-hop neighbors reply with REP message consisting of its ID and time of expiry and nonce sent by the receiver encrypted with the public key of the sensor node.

$$REP: \{ ID_{u_i}, [t_{exp}, nonce]_{K+_{a_j}} \}$$

  Receiving the REP messages from the sensor nodes, each privileged nodes make a list of its one-hop neighborhood with the s_{id} provided by the sensor nodes. The s_{id} is the id of sensor nodes provided by them in the REP message. This list helps the privileged nodes to cluster the sensor nodes. For

further communication, the sensor nodes willing to send data will send the message along with its certificate to the privileged node and privileged node will further provide privileged-to-privileged communication to transmit the message to a sensor node that does not belong to its own cluster.
Moreover, the cryptographic keys will help the network to avoid any maliciousness in between as data will be encrypted by the keys as necessary.

$$u_i \rightarrow a_j : \{[M]_{K-_{aj}}, Cert_{u_i}\}$$

$$a_j \rightarrow a_{j+1} : \{[M]_{K-_{aj}}, Cert_{u_i}, Cert_{a_j}\}$$

$a_{j+1} \rightarrow a_{j+2} : \{[M]_{K-_{aj+1}}, Cert_{a_j}, Cert_{a_{j+1}}\}$ and so on…….

Privileged nodes acts like the cluster head of their clusters and provide inter-cluster communication in network for sensor nodes. Clustering shows the distributed nature and operation of the algorithm.

- **Phase III: Wormhole Detection**

Detection of wormhole will lead by calculating the density of network. Once the neighborhood discovery is completed, then algorithm checks for any wormhole existence. The total area of the network is indicated by: $\mathcal{A}$, the total number of sensor nodes in the network is represented by: $\mathcal{N}_S$ and total number of privileged nodes are considered as: $\mathcal{N}_A$. Therefore, the network density becomes as:

$$\mathcal{D} = \frac{\mathcal{N}_S + \mathcal{N}_A}{\mathcal{A}}$$

We have also considered a threshold (Th) value for the wormhole detection which will help to calculate the closeness of the nodes and calculated as:

$$Th = \mathcal{A}_t . \mathcal{D}$$

Where, $\mathcal{A}_t = 2\pi R^2 - 2(2\pi R^2 . \frac{\alpha}{2\pi} - d.R.\sin\frac{\alpha}{2})$ shown in figure below with shaded region, which shows the area covered by threshold value. Where, $d = \frac{1}{2}\rho\sqrt{Th_c}$, $0 \leq \rho \leq 1$ defined as distance between the centres of two nodes A and B; and R is the average transmission range of the privileged nodes, d is the distance between privileged node and sensor node. Th_c is threshold value of closeness given as: $\frac{\mathcal{A}}{\mathcal{N}_S + \mathcal{N}_A}$.

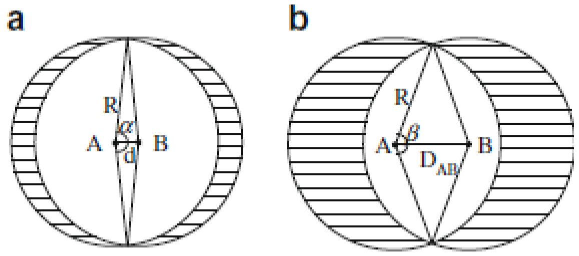

Figure 1. Wormhole Detection

If the value of closeness of nodes are greater than the threshold value for closeness of nodes, then there exists the wormhole nodes. Otherwise, no wormhole exists.

Copyright ⓒ 2017 SERSC

4. Simulation and Results

For the collection of results and proves for effectiveness of our proposed approach, we use simulator called Network Simulator version 2, because of its high clarity of modeling networking concepts. For the simulation purpose we use some set of simulation parameters:

Simulation Area	500 X 500
Routing Protocol	ZRP
Number of nodes	8
Antenna Model	Omni Antenna
Interface Queue Type	Priority Queue
Network Interface Type	Wireless Phy
Radio Propagation Model	Two Ray Ground
Channel Type	Wireless Channel

Table 1. Simulation Parameters

Performance Parameters: We set three parameters to testify the efficacy of our proposed algorithm as these ra the most affected parameters under wormhole attack:

- **Delay:** The delay will show the total delay encountered by the nodes under the wormhole attack in seconds. To find delay, we use formula:

  $$D = P_d + Q_d + T_d$$

  Where, P_d is processing delay that is time a node takes to process a packet, Q_d is the queuing delay that is the time a packet spent in the network queues and T_d is the transmission delay that is the time a packet take to transmit from source to destination.

- **Throughput:** The throughput refers to the maximum performance a node is capable of giving. The processing time without any faults are at a node will show its throughput. To show network throughput, we can take average of all node's throughput present in the network.

  T = number of processed packets/ latency for processing each packet

- **Packet loss ratio:** The packet loss ratio is the probability that how many packets get lost in the network under wormhole attack.

  PLR = number of packets lost / total number of packet received

Simulation Setup: In simulation environment we use an area of 500 X 500 and use ZRP protocol for routing decisions. We use three different radio ranges that is 5, 10 and 15. In results, the yellow wave will show the performance under wormhole existence. The red wave will show the performance at radio range 15, the green wave will show the performance at radio range 10 and blue wave will show the performance at radio range 5.

Results: After simulation we are having our results in X-Graph on the three performance parameters that is delay, throughput and packet loss ratio.

- **Case I: Packet Loss Ratio**

  The packet loss ratio is high with low radio range and low with medium radio range. But no significant changes in results of high radio range and wormhole affected scenario.

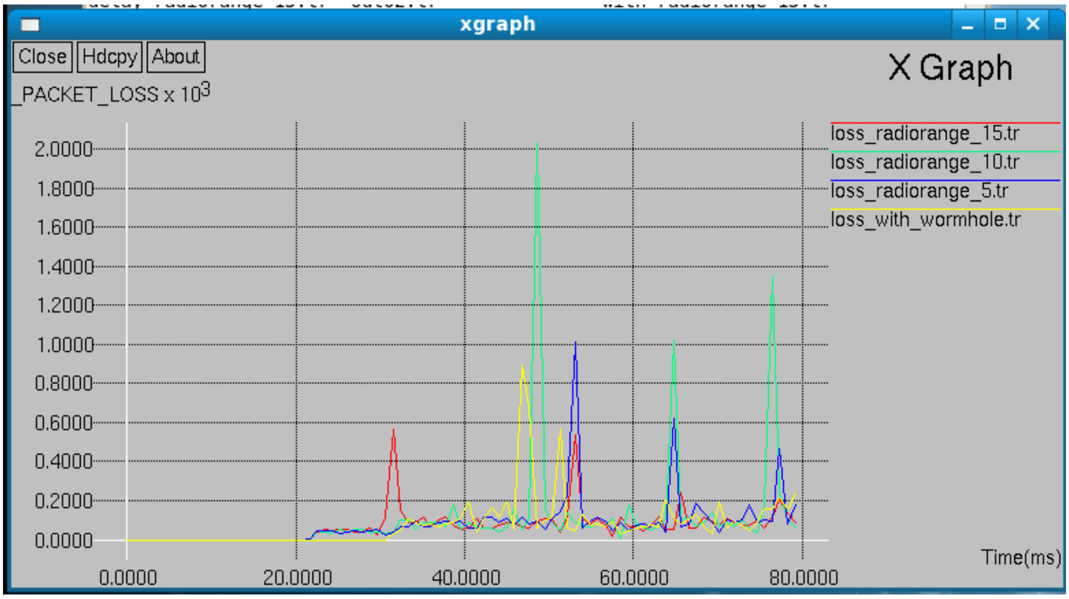

Figure 2. Packet Loss Ratio

- **Case II: Delay**

  When the radio range is less or is 5tr then the delay is very high. Under wormhole attack the delay is almost equal to the delay at radio range 5. The delay for radio range 10 shows quite less delay. The delay at radio range 15 is also burdensome.

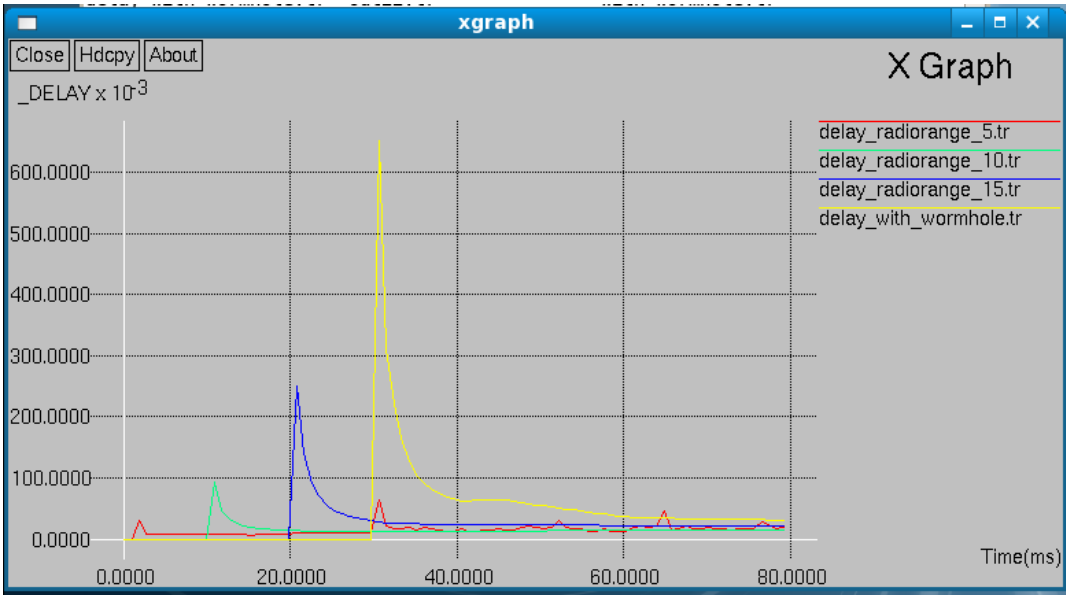

Figure 3. Delay

- **CASE III: Throughput**

  In case of high radio range throughput is high, then inline is medium radio range followed by low radio range and in wormhole the throughput affects the most.

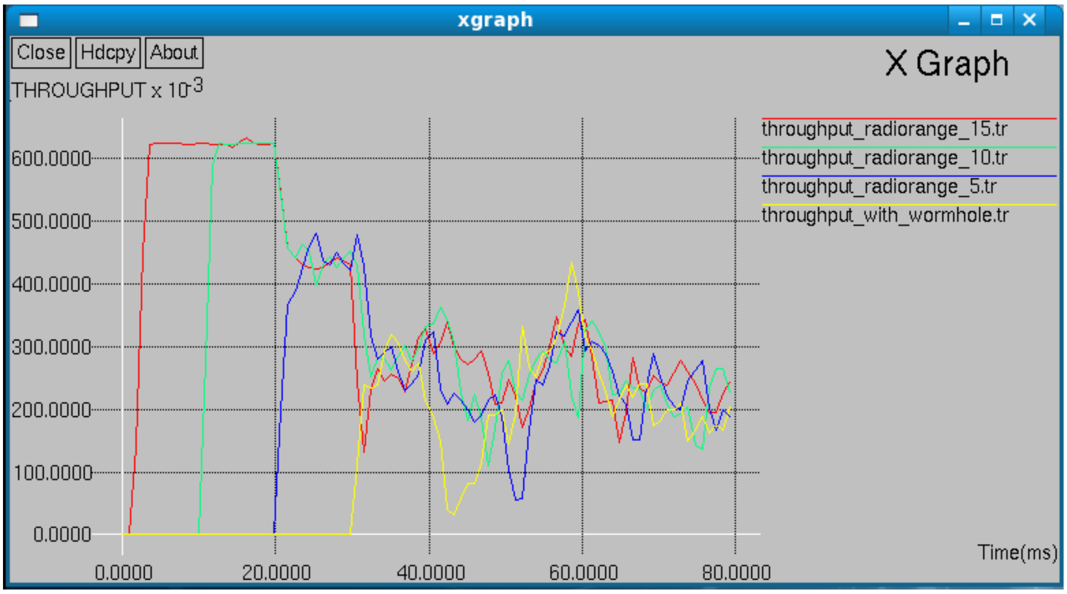

Figure 4. Throughput

The delay in wormhole is large, the throughput affected badly and packet loss ratio obviously increased. Delay is other parameter which tell us the optimality and effectiveness of schemes, lesser the delay more effectiveness. The more the throughput will be, the more effective the scheme will be. The computation overhead arises when schemes involves lots of calculations, if more overhead than more the delay and less effective. Some schemes require periodic updates for their smooth functioning but can degrade performance of network by increasing load on network. The false positive is a factor which might approve the malicious node in the network as a valid node, which is very harmful to network. The number of false positive should be less to prove the effectiveness and optimality of a scheme. The cryptographic mechanism is required for authentication the nodes present in network.

5. Conclusions

In the conclusion, we came to know that the proposed scheme or methodology is very effective in detecting the wormhole attack in wireless sensor networks. The proposed work follows a distributed approach as clustering is implemented. This scheme does not use any of the additional resources like highly synchronized clocks, location based hardware or software, high computational processors, etc. These are refrained to use in our proposed work. Also the processing of message packets involve little overhead. As the need of an hour for a distributed approach, our work fulfil the need. In future we can also try to use other feature than density feature for detection of wormhole attack in wireless sensor networks.

References

[1] C. Networks, “Wireless sensor network survey,” no. August 2008, **(2014).**

[2] M. Sowmya and K. Srinivas, “Literature Survey on Wireless Sensor Networks,” vol. 3, no. 6, **(2014)** , pp. 1093–1095.

[3] D. Carman, P. Kruus, and B. Matt, “Constraints and approaches for distributed sensor network security (final),” *DARPA Proj. Rep.*, **(2000)**, pp. 1–139**.**

Copyright ⓒ 2017 SERSC

[4] A. Bagula, “Applications of Wireless Sensor Networks”, **(2012)**, pp. 1–67.

[5] M. Messai, “Classification of Attacks in Wireless Sensor Networks,” *Icta*, (**2014)**, pp. 23–24**.**

[6] P. Maidamwar and N. Chavhan, “A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network,” *Int. J. Ad hoc Netw. Syst.*, vol. 2, no. 4, **(2012)**, pp. 37–50**.**

[7] S. Ughade, R. K. Kapoor, and A. Pandey, “An Overview on Wormhole Attack in Wireless Sensor Network : Challenges , Impacts , and Detection Approach,” vol. 2, no. 4, **(2014)**, pp. 105–110.

[8] R. Singh, “Countermeasures Against Wormhole Attack in Wireless Sensor Networks: A,”, vol. 6, **(2016)**, pp. 79–84.

[9] N. Jain, S. Gupta, and P. Sinha, “Clustering Protocols in Wireless Sensor Networks: A Survey,” *Int. J. Appl. Inf. Syst.*, vol. 5, no. 2, **(2013)**, pp. 41–50**.**

[10] P. Boora and S. Malik, “Performance Analysis of AODV , DSDV and ZRP Routing Protocols in WSN using Qualnet,” vol. 4, no. 6, **(2015)**, pp. 557–565**.**

[11] S. Kaur and S. Kaur, “Analysis of Zone Routing Protocol in MANET,” *Int. J. Res. Eng. Technol.*, vol. 2, no. 9, **(2013)**, pp. 520–524**.**

[12] S. Chang, I. Member, and I. C. Context, “A Fault Tolerance Spider-Net Zone Routing Protocol for Mobile Sinks Wireless Sensor Networks,” vol. 3, no. 4, **(2013)**.

[13] G. Padmavathi, P. Subashini, and M. D. D. Aruna, “ZRP with WTLS Key Management Technique to Secure Transport and Network Layers in Mobile Adhoc Networks”, vol. 4, no. 1, **(2012),** pp. 129–138**.**

[14] P. Amish and V. B. Vaghela, “Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol,” *Procedia Comput. Sci.*, vol. 79, **(2016)**, pp. 700–707**.**

[15] N. N. Dangare and R. S. Mangrulkar, “Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network,” *Procedia Comput. Sci.*, vol. 78, pp. 342–349, **2016.**

[16] W. Wang and B. Bhargava, “Visualization of wormholes in sensor networks,” pp. 51–60, **2004.**

[17] G. Akilarasu and S. M. Shalinie, “Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks,” *Wirel. Networks*, **(2016)**, pp. 1–10.

[18] T. Hayajneh, P. Krishnamurthy, D. Tipper, and A. Le, “Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies,” *Mob. Networks Appl.*, vol. 17, no. 3, **(2012),** pp. 415–430.

[19] T. Dimitriou and A. Giannetsos, “Wormholes no more? Localized wormhole detection and prevention in wireless networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6131 LNCS, **(2010)**, pp. 334–347.

[20] X. Ban, R. Sarkar, and J. Gao, “Local connectivity tests to identify wormholes in wireless networks,” *Proc. Twelfth ACM Int. Symp. Mob. Ad Hoc Netw. Comput.*, , **(2011)**, p. 13:1--13:11.

[21] Y. Ravikumar and S. Chittamuru, “A Case Study on MANET Routing Protocols Performance over TCP and HTTP,” *Sch. Eng. Blekinge***, (2010)**.

[22] G. Kumar, M. K. Rai, H.-J. Kim, and R. Saha, "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks", Article ID 3243570, **(2017)**, pp. 1-12.