# An Efficient Cluster-Based Approach to Thwart Wormhole Attack in Adhoc Networks

Kollu Spurthi[1]
Research Scholar, Department. of Computer Science and Engineering, KLEF, AP, India

Dr.T N Shankar[2]
Associate Professor, Department. of Computer Science and Engineering, KLEF, AP, India

***Abstract*—Mobile Ad-hoc networks is an ascertaining domain with promising advancements, attracting researchers with a scope of enhancements and evolutions. These networks lack a definite structure and are autonomous with dynamic nature. The strength of the Ad-hoc network lies in the routing protocols making it an apt choice for transmission. With several types of routing protocols available our focus is on LGF (Location-based Geo-casting and Forwarding) protocol that falls in Position based category. LGF assures to grab the attention with its feature of low bandwidth consumption and routing overhead at the cost of unvolunteered attacks resulting in compromising the security of data. In our approach, we present a technique to overcome the profound attacks like Wormhole and Blackhole by aggregating LGF with k++ Means Clustering aiming at route optimization and promoting security services. The proposed mechanism is evaluated against QoS factors like End to End delay, Delivery Ratio, Load balancing of LGF using Simulator NS3.2 which envisioned drastic performance acceleration in the aforementioned model.**

***Keywords*—MANET; LGF; K++ Means clustering; network security; wormhole attack; blackhole attack; secured algorithm**

## I. Introduction

MANETs, a group of nodes that provide communication through wireless links without a predefined infrastructure and exhibiting dynamic nature has been the choice of practitioners and researchers for two long decades. The ad-hoc feature of MANETS makes it a favorable choice in several applications like Vehicular communication handling various disaster scenarios, defense, Security, and Online meetings. These applications depend on information exchange between nodes that play a vital in the process of Communication. The Crucial component acting as the backbone for node elucidation and improving the strength of MANETS ate routing protocols. It is a syntactic rule for defining a methodology to be undertaken by routers for transmission of data.

Based on the consideration surveyed by various researchers these protocols are classified as Topology based and Position-based. The former protocols rely on the respective structure of the network, whereas the latter originate with the location information of nodes. Topology based routing protocols fall into three well-known models like Proactive, Reactive, and Hybrid. Proactive protocols as the name reflect works based on prior information stored in the table in contrast reactive build a route on-demand when a request triggers. Bridging the gaps among both Hybrid protocols intersects the characteristics of Proactive and Reactive [24]. Few well-known protocols falling on the Proactive side are DSDV, FSR, OLSR, and reactive are AODV, DSR, and TORA. ZRP, ZHLS, CEDAR are occupied under hybrid Class [23]. These protocols fail to outperform when the network turns to be densely populated with a huge number of nodes resulting in large network sizes, thereby lowering performance [20]. To leverage and sustain the network efficiency even with dense networks, MANETS impend on position-based routing protocols with urging requirement of security features [15]. Few protocols of interest are namely LAR, LGF, and Landmark. SLAR is also proposed to provide security against different attacks [16]. These protocols ensure efficient performance when clustered into zones [4]. Position based class mainly emphasizes the position of the node in the network and their performance is analyzed based on qualitative characteristics like Loop free, Decentralized operations, Path strategy, Performance metrics, Scalability, Reliable Delivery service, and Robustness. These Protocols support few strategies in packet forwarding namely Greedy Forwarding, Constrained directional flooding, and additionally Hierarchical or multilevel methods [2]. The greedy method of forwarding works by using optimization criteria for selecting the next node for the transmission of messages [22]. With directional flooding sender floods, packets to nodes toward the direction of destination satisfying predefined constraints and the Hierarchical method works when huge network scaling is on-demand [26].

Among several position-based routing protocols, our focus is on LGF that targets the reduction of routing overhead and bandwidth. In LGF the neighboring nodes in the forwarding zone perform rebroadcasting route request packet and acknowledge the source with route reply. Unlike all routing protocols, LGF is also vulnerable to serious attacks like Wormhole and Blackhole attack. These attacks exhibit an adverse impact on the performance of location-based ad-hoc networks [8].

Our paper enlightens all the fore-mentioned issues and proposes an enhanced approach based on the K++ Clustering technique to overcome attacks in LGF.

## II. Related Work

Ahmad, Hameed, & Ikram, 2019, analyzed Ad-hoc networks and came up with a unique cluster-based algorithm for a reduction in the size of the routing algorithm. AI-Shrugan, Ghazali, & Hassan, 2012, gave a qualitative comparison of the position-based protocol in the context of the

greedy forwarding strategy. Alinci, Spaho, Lala, & Koli, 2015, reviewed MANETS related to clustering schemes like mobility-based, Energy-based connectivity with their pros and cons. Amouris, Papavasilliou, Maaloi, 1999, designed a protocol based on location routing zones which is efficient in the utilization of bandwidth for the huge size of networks. Dyabi, Hajami, & Allali, 2014, proposed the MANET clustering algorithm based on node density for cluster head selection. This approach promises improved results. Farjamnia, Gasimov, & Cavanshir, 2019, contributed a detailed review of handling the wormhole and analyzed its effect on the wireless network. Gayatri, et al., 2019 discussed in detail the wormhole attack in AODV and analyzed the framework by tracking the high transmission node. Giordano, Stojmenovic, 2004, presented a clear taxonomy on position-based routing models in Adhoc networks. Gupta, Singh, 2016, contributed a detailed study on wormhole attacks in wireless networks. Hamad, Kang, Jeon, & Nam, 2008 contributed to K-Means clustering in RDMAR protocol using the distance between nodes. Hossian et al., 2019 put a ray of light on the detection of a black hole in AODV and AOMDV adopting fusion of SHA-3 and Diffie-Hellman. Joo-Han song, et al., 2007 contributed the Secure Geographic Forwarding technique and SGLS with LRS (Location Reputation System) and comparison of their performance analysis. Kulkarni, Bukate, & Nanaware, 2018, provided an immense study on different attacks in Manets. Lattif, Ali, Ooi, & Fisal, 2005, proposed a detailed description of LGF implementation in MANETS with the GPS-FREE mechanism. Mahmood & Manivannan, 2018, discussed on Greedy Routing Protocol related to backtracking and compared performance issues with AODV and DSR protocol. Moudini, Er-Rouidi, Mouncif, 2016 evaluated secure Adhoc routing protocols categorized them into three types, and analyzed different protocols for secured and efficient routing in MANETS. Muthupriya, Revathi, & Rahman, 2017, designed a new algorithm SLAR enhancing security in LAR protocol against various types of malicious nodes. Patel A, Patel N, Patel R, 2015, proposed a Hash-based compression function based on a hash function for the RREQ packet with promising results. Priya Maidamour, Nekita chavan, 2012 surveyed and analyzed the vulnerable security threats like the Wormhole attack. Mishra, Gandhi, & Singh proposed a weighted forward method that is a fusion of forwarding, selection schemes of a node within a predefined area. Rajkumar Kapur, & Sunil Kumar Khatri, 2015, provided a detailed analysis of several vulnerabilities on routing protocols. Razaee, Yaghmaee, 2014, analyzed on cluster stability and proposed a Weight based algorithm for nodes with enhanced results. Royer, Toh Chai-Keong, 1999, reviewed about eight routing protocols, their functions, advantages, disadvantages, and provided a detailed comparison between these protocols, which helped our work in getting deeper. Sumit, Mitra, & Gupta, 2014, proposed an effective K-Means clustering and implemented IDS in MANETS using ZRP to avoid malicious activity. Srivastava, Daniel, Singh, & Saini, 2012, proposed a protocol for Energy Efficient Position-based routing with two new methods for route maintenance in Ad-hoc networks. Teotil, Dhurandher, Woungang, & Obaidat, 2015, proposed the COTA Approach in Position-Based Routing Protocol LAR1, which showed efficiency in terms of security against the Wormhole attack. Yih-Chun Hu, Perrig, & Johnson, 2006, came up with a TIK protocol to handle Wormhole Attack in MANETS.

## III. Existing Approach

LGF: LGF with its beneficiary factors like lowering bandwidth and packet dropping rises to be the best choice for leveraging performance about measuring concerns like efficient packet forwarding in MANET's. Steps involved in LGF include path discovery and message forwarding [13, 22].

- The process initiates from a source with a multicast PREQ packet to all neighboring nodes based on the IP address of the destination. The protocol limits its range within a predefined distance.
- RREQ packet is forwarded to all the neighboring nodes with a distance less than the source node to the destination.
- The process repeats until the RREQ packet reaches the destination that further acknowledges the path to the source node from various intermediate nodes.
- Finally, the optimal shortest path is captured, and intended packets are transferred among source and destination.

Despite limitations with LGF when the range increases, it also suffers from a Wormhole attack that targets the shortest path with an illusion perspective. To handle this perturbation our algorithm fusions LGF with a clustering approach resulting in a secure, reliable transmission.

### A. Attacks on ad-hoc Networks

An attack aims at compromising the security of transmission innumerable ways like Interruption, Interception, modification, Fabrication, or denial of service. A Wireless network is mainly prone to such type of attacks due to their dynamic nature [22]. Based on the method of disrupting security services [11], attacks are characterized by direct manipulation to the transmitted data, conversely passive as eavesdropping the communication between the parties [12]. Many attacks are figuring out, of which Wormhole attack and Black hole are considered [13,7].

### B. Impact of Wormhole Attack

Limited availability of resources dispenses Ad-hoc network to attacks. An unauthorized entity with high power supply, memory, and computational capability is successful in introducing malicious attacks over MANET's [6].

A Wormhole attack is one worth enough to affect the network without revealing the cryptographic mechanisms embedded [9]. This attack has two variations that are hidden and exposed [29, 18].

*1) Hidden wormhole attack*: In this scenario the attacker succeeds in hiding the identity of the nodes between source and destination, creating an illusion of source and destination as one-hop neighbors [25].

*2) Exposed wormhole attack:* Here the attackers introduce themselves into the network with route discovery technique,

thereby exposing Wormhole nodes and hiding liable nodes between source and destination [28]. Based on these modes different forms of Wormhole attacks are-encapsulated packet-based, Wormhole attack, out-of-band path, relaying of packets, and Protocol manipulation wormhole attack [21].

### C. Black Hole Attack

A serious problem endeavoring wireless sensor networks is the Blackhole attack characterized to absorb everything that comes on the way thereby decreasing the performance of the network [17]. In this attack, a malicious node or attacker node announces that it indexes the shortest path to the destination resulting in packet loss. It succeeds in communication failure among wireless networks and base stations. This attack results in topology modification including packet damage with forged routing information [23,10].

## IV. Proposed Approach

### A. Lgf with Clustering Approach

As LGF is prone to several attacks discussed and even restricted with range constraints. We propose a variation of LGF in combination with the clustering technique to handle the demerits of LGF. K++ Clustering is embedded in our proposed mechanism to strengthen the LGF for overriding the deficiencies [11].

K++ Means: This algorithm aims at clustering the given dataset into clusters and mainly focuses on seed or initial value selection, as an input to k-means. It overcomes the poor Clustering results of K-means which is an NP-hard problem. K-means gives the worst results for super polynomials in input and bad approximation of objective function in comparison with optimal clustering [5] that is overridden in k++ by the defined procedure to initial Clusters [1,3].

Step by Step Procedure for k++ is given as:

*1)* Select a data point C randomly.

*2)* For every data point P, Calculate the distance d(p) between P and C.

*3)* Pick a new data point based on weighted probability distribution with n proportional to $d(p)^{2.}$

*4)* Iterate steps 2 and 3 until optimal k centers are selected.

*5)* Continue with k-Means Clustering after the initial seed value is selected [27].

Position Based Protocols by virtue depends on the location of the node which ascertains performance assurance. These Protocols rely on three main sources to identify the exact location of the nodes, namely, based on signal strength, coordinates between nodes, and GPS based node location. Our approach uses the coordinates to locate the point of the node which helps in identifying malicious node location that promotes traffic bypassing within the network.

### B. Phases in Proposed Approach:

Phase1: The network is divided into clusters using the k++ Clustering technique, resulting in k value. The source node initiates the RREQ packet for route discovery when a communication link is needed. This RREQ packet is forwarded to the nearest neighbors with the shortest Euclidean distance.

Phase 2: In this Phase Destination Node acknowledges the RREQ packet with RREP through the shortest path opted. The legitimacy of the RREP packet is judged or evaluated based on the predefined threshold value of RREP packets permitted.

Phase 3: Here a node is considered malicious once it violates the threshold value constraint of the RREP packet. The path the malicious node resides is excluded from the transmission path for forwarding packets. This phase also checks the hop count in the routing table to identify the path established by the hidden malicious node.

Our procedure succeeds in overcoming the Range constraint using k++ and Node Authentication by considering the location of the node as criteria using coordinates for calculating the Euclidean distance. Euclidean distance also adds to overcome the shortest path illusion injected by Wormhole and Black attacker nodes with the help of the RREP packet threshold value.

### C. Algorithm for Clustering enhanced LGF

There are some descriptions as given below to recover a safe RREP Packet through intermediate nodes.

Assume source node value = 1 and 2.
Intermediate nodes value = 1, 2.
Hop count node value = 3.
If (source node value == intermediate nodes value 1and 2)
{
Accept the RREP packet to the source node.
}
Else
{
The Source node discards the RREP packet because it is malicious node paths.
}
3. With this condition as benchmark source node waits and checks for safe route reply RREP packet through the intermediate nodes.

**// location selection of node using k++ means**

Require: k++means Function(cluster :list)
for k++meansFunction(cluster : list)
do Xk ← Xk + cluster.X
Yk ← yk + cluster.y
end for
XK ← XK /long(cluster)
YK ← YK /long(cluster)
N ← N − 1 return (XK,YK)

**// selection of cluster (based on the location of a node)**

Require: k++means Function(cluster :list)
for (ifrom1tolong(Cluster))
do X ← Cluster.X
Y ← Cluster.Y
distance = sqrt((Xk − X) ∗ (Xk − X) + (Yk − Y) ∗ (Yk − Y))
if (distance < distancemin) then
distance min=distance end if end for return (distancemin)

## V. Performance Evaluation and Analysis

To Implement the Proposed approach using NS3.2, the Simulation parameters are initialized as shown in Table I. The performance of LGF with K++ Means is evaluated by considering the parameters like Load Balancing, End to End Delay, and Delivery ratio.

*1) End to End delay:* End to End delay is defined as the time incurred to travel from source to destination [19].

*2) Packet delivery ratio:* This is the ratio of the number of packets delivered to the number of packets sent by the source node [14].

*3) Load Balancing:* A parameter that defines an efficient distribution of transmission load during transmission in a network.

Fig. 1 shows a clear comparison of the reduced End to End delay factor proposed in comparison to the existing system. Here proposed system is indicated as lgfc-delay with a green spike.

Fig. 2 shows a comparison of the Delivery ratio which shows the packet loss of the Proposed and Existing system. Here proposed system Promises a reduced packet loss with a green spike.

TABLE I. Simulation Parameters

| PARAMETERS | VALUES |
|---|---|
| *Simulator* | *NS 3.2* |
| *Simulator Time* | *120 s* |
| *Simulation Area* | *1000*1000 m* |
| *Proposed Protocol* | *LGF-C(hybrid approach)* |
| *Initial Energy of nodes* | *1J* |
| *Number of Nodes* | *22* |
| *Bit Rate* | *1Mb/sec* |
| *Packet Length* | *600 byte* |

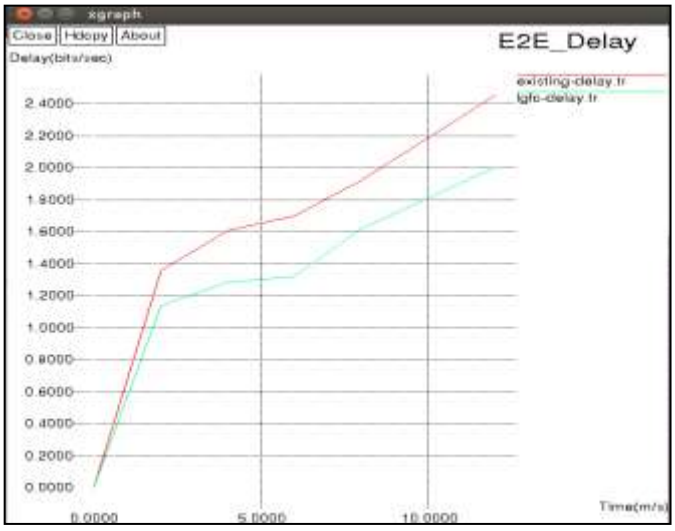


Fig. 1. Graph Showing End-To-End Delay.


Fig. 2. Graph Showing Delivery Ratio.


Fig. 3. Graph Showing Load Balancing Factor.

Fig. 3 shows a comparison of the load balancing factor which projects a better performance by the pfroposed system of lgfc indicated with a green spike.

Hence the simulation results of the proposed protocol outperform in terms of End to end delay, load Balancing, and in the reduction of Packet Loss by providing node authentication, Reliability and stability thereby leveraging the performance of the network in Position-Based Routing Protocols.

## VI. Conclusion

This paper aimed to discuss the importance of MANETS and concentrated on the adverse effects of Wormhole and Blackhole attacks in the position-based routing protocol. LGF Protocol is studied for various setbacks related to delivery, avoiding Attacks, and providing Authentication of nodes with Location as a constraint. Our approach is considered a clustering-based method to overcome the Prior mentioned issues in LGF with enhanced K++ Mean's supporting attack free and secure packet transmission in Wireless Ad-hoc Networks.

REFERENCES

[1] M. Ahmad, A.Hameed, A. Ikram, & I. Wahid, " State of the art clustering schemes in mobile ad hoc networks: objectives, challenges, and future direction", IEEE Access, DOI:10.1109/access.2018.2885120, 2018.

[2] M. Al-Shugran, O. Ghazali, & S. Hassan, "Performance Comparison of Position-Based Routing Protocols in the Context of Solving Greedy Failure", International Conference on Advanced Computer Science Applications and Technologies (ACSAT). DOI:10.1109/acsat.2012.20, 2012.

[3] M. Alinci, E. A. Spaho, A. Lala, & V. Kolici, "Clustering Algorithms in MANETs: A Review", Ninth International Conference on Complex, Intelligent, and Software Intensive Systems. DOI:10.1109/cisis.2015.47, 2015.

[4] K. N. Amouris, S. Papavassiliou, & Li. Miao (n.d.), "A position-based multi-zone routing protocol for wide-area mobile ad-hoc networks", IEEE 49th Vehicular Technology Conference (Cat. No.99CH36363). DOI:10.1109/vetec.1999.780570,1999.

[5] M. Dyabi, A. Hajami, & H. Allali, "A new MANETs clustering algorithm based on nodes performances", International Conference on Next Generation Networks and Services (NGNS). DOI:10.1109/ngns.2014.6990222, 2014.

[6] G.Farjamnia, Y.Gasimov & K.Cavanshir "Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Networks", Wireless Personal Communications, volume 105, pages1561–1584,

[7] S. Hossain, M. S. Hussain, R. R Ema, S. Dutta, S. Sarkar, & T. Islam, "Detecting Blackhole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET", 10th International Conference on Computing, Communication and NetworkingTechnologies(ICCCNT), DOI:10.1109/icccnt45670.2019.8944395, 2019.

[8] S. Gayathri, R. Seetharaman, L. H. Subramanian, L. H., Premkumar, S., Viswanathan, S., & Chandru, S, "Wormhole Attack Detection using Energy Model in MANETS",2nd International Conference on Power and Embedded Drive Control (ICPEDC). DOI:10.1109/icpedc47771.2019.9036536, 2019.

[9] N. Gupta, & S. N. Singh," Wormhole attacks in MANET", 6th International Conference - Cloud System and Big Data Engineering (Confluence). DOI:10.1109/confluence.2016.7508120, 2016.

[10] O. F. Hamad, M.Y. Kang, J.H. Jeon, & J.S. Nam, "Neural Network's k-means Distance-Based Nodes-Clustering for Enhanced RDMAR Protocol in a MANET,".IEEE International Symposium on Signal Processing and Information Technology. DOI:10.1109/isspit. 2008.4775666, 2008.

[11] R. K.Kapur, & S.K.Khatri, " Analysis of attacks on routing protocols in MANETs", International Conference on Advances in Computer Engineering and Applications. DOI:10.1109/icacea.2015.7164811, 2015.

[12] A. N Kulkarni, R. R Bukate, & S. D. Nanaware, "Study of Various Attacks and Routing Protocols in MANETS", International Conference on Information, Communication, Engineering and Technology (ICICET). DOI:10.1109/icicet.2018.8533696,2018

[13] L. A.Latiff, A.Ali, Chia-Ching Ooi, & N.Fisal, "Location-based geo casting and forwarding (LGF) routing protocol in mobile ad hoc network", Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05). DOI:10.1109/aict.2005.55,2005

[14] B. A.Mahmood, & D.Manivannan,"GRB: Greedy Routing Protocol with Backtracking for Mobile Ad-Hoc Networks", IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems. DOI:10.1109/mass.2015.49,2015

[15] H. Moudni, M. Er-round, H. Mouncif, & B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks", International Conference on Information Technology for Organizations Development (IT4OD). DOI:10.1109/it4od.2016.7479295, 2016.

[16] V. Muthupriya, S. Revathi, & B. S. A. Rahman, "Secure Location Aided Routing (SLAR) for mobile ad hoc networks", IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). DOI:10.1109/icpcsi.2017.8392279, 2017.

[17] A.Nabou, M. D. Laanaoui, & M. Ouzzif, "Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3",6th International Conference on Wireless Networks and Mobile Communications (WINCOM). DOI:10.1109/wincom, 2018.

[18] A. Patel, N. Patel, & R. Patel, " Defending against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, DOI:10.1109/csnt.2015.253, 2015.

[19] PanelJoo-HanSong, Vincent.W.S.Wong, & Victor C.M.Leung "Secure position-based routing protocol for mobile ad hoc networks Ad Hoc Networks ", Volume 5, Issue 1, January 2007, Pages 76-86

[20] Priya Maidamwar, Nekita Chavan, "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network International Journal on AdHoc Networking Systems, volume 2 issue(4):37-50 · October 2012 DOI: 10.5121/ijans.2012.2404

[21] Priya Mishra, Charu Gandhi, & Buddha Singh, "An Improved Greedy Forwarding Scheme in MANETs Technology", JIIT, Noida, U.P., Ind, journal of telecommunications and information technology, pp. 50-55, 2017.

[22] Rajinder Singh, Parvinder Singh, Manoj Chavan "An effective implementation of the security-based algorithmic approach in mobile Adhoc networks", Human-centric Computing and Information Sciences, volume 4, Article number: 7 (2014)

[23] M. Rezaee & M. H. Yaghmaee, " A new clustering protocol for Mobile Ad-Hoc Networks", International Symposium on Telecommunications, DOI:10.1109/istel.2008.4651331, 2008.

[24] E. M. Royer & Toh Chai-Keong, " A review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications, 6(2), 46–55. DOI:10.1109/98.760423, 1999.

[25] S. Giordano, I. Stojmenovic, " Position-Based Routing Algorithms For Ad hoc Networks: A taxonomy", Ad Hoc Wireless Networking, pp 103-136, volume 14, 2004.

[26] S. Srivastava, A. K. Daniel, R. Singh, & J. P. Saini, Energy-efficient position-based routing protocol for mobile ad hoc networks. 2012 International Conference on Radar, Communication, and Computing (ICCRC), DOI:10.1109/icrcc.2012.6450540, 2012.

[27] S. Sumit, D. Mitra, & D. Gupta, " Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining", International Conference on Reliability Optimization and Information Technology (ICROIT), DOI:10.1109/icroit.2014.6798303, 2014.

[28] V. Teotia, S. K. Dhurandher, I. Woungang, & M. S. Obaidat, " Wormhole prevention using COTA mechanism in position based environment over MANETs", IEEE International Conference on Communications (ICC), DOI:10.1109/icc.2015.7249448, 2015.

[29] Yih-Chun Hu, A. Perrig, & D. B. Johnson, " Wormhole attacks in wireless networks", IEEE Journal on Selected Areas in Communications, 24(2), 370–380, DOI:10.1109/jsac.2005.861394, 2006.