I. J. Computer Network and Information Security, **2019, 5, 20-27**
Published Online May 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.05.03

Distributed Wormhole Attack Mitigation Technique in WSNs

Sharada Kori
KLS Gogte Institute of Technology, Department of CSE, Belagavi, Karnataka, India
E-mail: smkori@git.edu

Dr. Krishnamurthy G N
Department of CSE, BNM Institute of Technology, Bangalore, India
E-mail: krishnamurthy_gn@hotmail.com

Dr. Nandini Sidnal
Department of CSE, KLE CET, Belagavi, India
E-mail:sidnal.nandini@gmail.com

Received: 19 February 2019; Accepted: 20 March 2019; Published: 08 May 2019

***Abstract*—**Sensing element Networks area unit gaining a lot of attention as a result of applications like sensible cities(traffic congestion, sensible parking, sensible lighting), sensible setting (forest hearth detection, air pollution) security and emergencies (Radiation levels, Explosive and dangerous Gases, Military applications) to call a couple of. The important facet of those observation and chase applications area unit security and sensing element location. The Wireless sensing element Networks may be thought to be associate degree freelance theme for accomplishing data-intensive chores like atmosphere (habitat) perceptive, data congregation, earthquake perceptive, parcel intelligence operation, etc. and any communication to the appliance. Wormhole attack could be a severe threat to the safety of the network. Because it could be a passive attack, it's terribly difficult to notice Wormhole attack. The most stress of this analysis work is to mitigate the wormhole attack. During this paper, we have a tendency to address the wormhole attack by proposing a trust-based wormhole attack mitigation technique. Our projected system is easy with no further hardware demand and no tight clock synchronization.

***Index Terms*—**WSN, Security, Wormhole Attack, Wormhole attack mitigation.

I. Introduction

Sensor Networks are gaining additional attention owing to applications like good cities (traffic congestion, good parking, good lighting), good setting (forest hearth detection, air pollution) security and emergencies (Radiation levels, Explosive and dangerous Gases, Military applications) to call a number of. The crucial side of those observance and pursuit applications are security and device location.

The Wireless device Networks are often considered associate degree freelance theme for accomplishing data-intensive chores like atmosphere (habitat) observant, data congregation, earthquake observant, field of honor intelligence, etc. and more communication to the appliance.

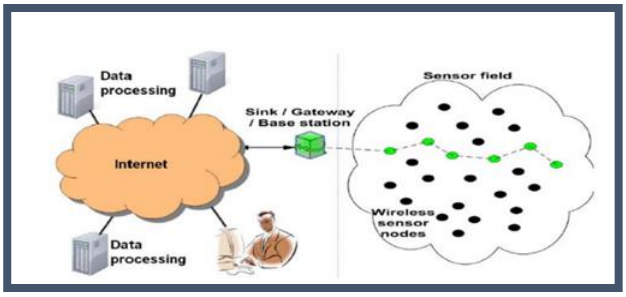

Fig.1. Architecture of a typical Wireless Sensor Network

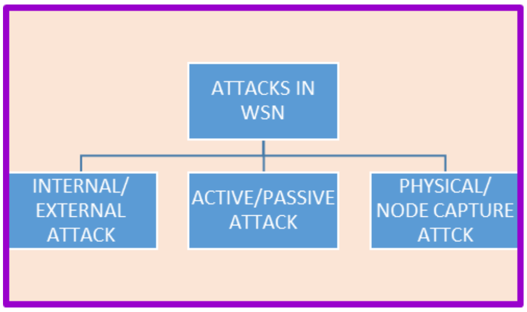

Fig.2. Attacks in WSN

II. Related Works

A. *Security Issues in Wireless Sensor Networks*

WSNs are typically featured with the random preparation of nodes, communication among nodes via wireless links. No physical protection and restricted resources create it susceptible to differing types of intrusions. The intrusion in WSN is broadly speaking classified into 3 totally different classes as shown in figure 2. The attacks could also be internal/external, active/passive or physical/node capture attack. [6].

Internal/ External Attacks: In within attack, the inner node is compromised, has access to partial keys and have the boldness of detector nodes. In associate external attack, the offender merely injects facts or snoop on records to interrupt the everyday procedure of the system. Discovery of corporate executive attack is additional troublesome than foreigner attack.

Passive/ Active Outbreaks: Passive outbreaks are slightly spying kind and during this hot user makes an attempt to stay track of and follow up the communication. The active outbreaks are in control of key alterations of the knowledge or they'll create a particular fictional stream of information in a very WSN.

Physical Attack/Node Capture Attack: In physical intrusion, invaders gather the entire management on all the happenings happening via sensing element node. Invaders arrest the node themselves by mistreatment taking entire bodily access, therefore referred to as Physical attack [3, 4]. These outbreaks injury sensors lastingly, therefore the damages can't be in awe of. One technique to beat physical assault is Tamper proofing. However this approach is inappropriate in WSN.

*Attacks in various layers of Networks:*Attack (internal/external) could to boot seem at any layer of the community i.e., Physical layer (Eavesdropping, Jamming, Node Tampering), circuit layer (Intelligent jam, Collision), Network layer (Spoofing, Replay, Selective forwarding, Blackhole, Sinkhole, Wormhole, hi Flood), Transport layer (Data Integrity, Energy Drain) and Application layer (Reliability attack, Malicious code attack). This space focuses on quite an range of safety threats in WSNs at the network layer.

Network Layer Attacks: One essential practicality of the network layer is to transmit information from one node to a different. Invaders may to boot gain entree to transmission routes to omit on the positioning guests and deliver bound imperfect statistics regarding the pathway to WSN or they will gift Denial-of-Service outbreaks. Bound attacks taking neighborhood during this layer are as below:

- *Selective forwarding Outbreak:*

In Selective forwarding eruption, mischievous nodes truly drop packets that are alleged to be impaired and by selection transmits completely different packets which are of lesser activity [7]. In part eruption, node drips utterly all packets that it obtains.

- *Sybil Attack:*

In Sybil happening, a solo node tends to own varied individualities [7]. Sybil attack interrupts operating of geography routing policies via being at the identical time as at further than one habitation.

- *Sinkhole Outbreak:*

In the natural depression natural event, a mischievous node tends to be additional conspicuous, neighboring nodes try and transmit knowledge to the present malicious node presumptuous that it's one hop away [7]. Natural depression assault promotes selective forwarding attack because it attracts guests from all nodes.

- *Wormhole Attack:*

In wormhole irruption, ideally, 2 mischievous nodes structure a passageway within the network. The node at one side gathers packets from neighbors, transmits them with the help of tunnel to the malicious node at the opposite edge [5]. If messages transmitted between the tunnels are not changed, then wormhole attack is cooperative in quicker communication of information. However sometimes the foremost styles of packets are plunged and exclusively selective packets are communicated. An outsized form of nodes get attracted by victimization these malicious nodes thanks to the actual fact of speedy information transfer forward that they're one hop away. Within the worst case, if whichever mischievous node is near sink, then the massive movement is drawn through the malicious node. Figure.2, suggests however the wormhole irruption is launched between nodes S_2 and S9. It's quite difficult to watch natural depression assault and wormhole attack. These assaults are capable to beat through the resource of bound topographic sending conventions [6]

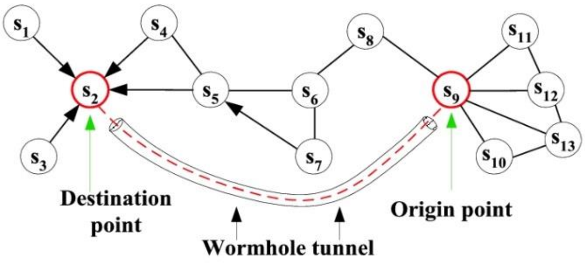

Fig.3. Wormhole Attack in WSN

Two adversaries produce a digital tunnel in hollow assault to scoop statistics transmission within the network. The shorter link is formed amongst adversaries at the tunnel half points. Hollow eruption could be a severe hazard to sensing element networks since this vary of outbreak cannot want cooperating a sensor within the system; in its place, it ought to be achieved even at the preliminary stage at some purpose of the sensors units to acknowledge its handy knowledge. These hollow outbreaks are very tough to stopover because of this reality routing fact given through a sensing element node is incredibly difficult to verify. The hollow eruption is perhaps through the encroacher has not cooperated with any of the nodes and though complete transmission affords privacy and is correct additionally.

III. Problem Identification

In a typical wormhole attack, a mischievous node captures traffic at one point of the tunnel and routes it to the other end of the tunnel, and there it is replayed. This impacts the route discovery process by thwarting nodes from determining genuine routes that are more than two hops away. Hence in this research proposal, we have planned to address the issue of mitigation of wormhole attack in a wireless sensor network based on certain authentication mechanisms. Invaders propose these channels as properly eminence paths to the sink. Therefore, adjacent sensor nodes take delivery of these channels into their transmission channel, decoding their data beneath the inquiry of the opponents. As quickly as the passageway is formed, the invader accumulate data packets on one terminal of the passageway, directs them by using the capability of the passageway (may be wired or Wi-Fi channels) and reiterates them at a different terminal. Wormhole outbreaks may want to impact in extreme harms in DSNs by means of disturbing or various the facts circulate en route for the base station. Along with this, if the invaders do no longer alter or produce facts packets, cryptographic way out single-handedly cannot perceive wormhole outbreaks. Protecting against such an outbreak is perplexing on the grounds that it can be thrown even if all community verbal exchange is honest and private.

Safety gap on hand to obtain wormhole outbreak:Sensor node credentials secrecy, sensor node locality secrecy, course secrecy and records packet secrecy [8] are certain secrecy primitives recognized for safe communication. These primitives' resource sensor nodes to shield their information. Then invader can easily seize the packets and snip refined statistics by means of cooperating a node in the system. By what means the wormhole outbreak is achieved:

Wormhole outbreak is achieved with the aid of two or additional malevolent nodes having most fulfilling assets than other sensors in the network. These malevolent nodes produce brief latency hyperlink (high bandwidth tunnel) [10] [9] amongst them. The channel can be recognized in several ways, such as through an out-of-band out of sight channel (e.g., a wired link), packet encapsulation or excessive power-driven communication. Later launching the channel, invader encourages these channels as finest paths to the base station. From this time, close by sensor nodes approve these channels into their communication routes, decoding their data below the inspection of the foes [11]. As soon as the channel is recognized, the invaders collect information packets on one termination of the channel, direct them via capacity of the channel (wired or wireless link) and reiterate them at the different termination. Wormhole outbreaks perchance will outcome in extreme harms in WSNs by means of intruding or altering the records movement en route for the base station.

Alternates of Wormhole Outbreak: Around three alternates of wormhole outbreak are possible: Black gap attack, Gray hole assault, and Sinkhole attack. They are classified in accordance with the ruthlessness of their thieving data and simplicity of discovery in the system.

- *Black hole Outbreak:*

Here in this kind of the wormhole outbreak, invader attempts to gather most information and then practice that facts and then drips it disadvantaged of merchandising to additional nodes [12]. Since it drops absolutely accessible records it is normal as Black gap attack. This is the modest and casual technique of wormhole outbreak. The disadvantage of this variety of outbreak is that it can easily be recognized by using the usage of facts go with the flow scrutiny and grid established practices.

- *Gray hole Outbreak:*

This is another choice of the wormhole outbreak and is smarter than the Blackhole outbreak. Just to lessen the likelihood of discovery, packet dropping in Gray hole outbreak is performed selectively [13]. Gray gap outbreak additionally exhibits arbitrary things to do [13] the place packet sinking is carried out arbitrarily, on the other hand, transmitting different packets. In this fashion making it extra difficult to discover the malevolent nodes. Consequently, it comes to be very difficult to discover the Gray gap outbreak, than Blackhole outbreak in the sensor system.

- *Sinkhole Outbreak:*

Sinkhole assault is the utmost hazardous and smart variant of the wormhole outbreak. In this outbreak, malevolent nodes collect the information, makes use of it and later it alters the statistics and then reiterates it in the sensor network [13]. In Sinkhole assault every so frequently malevolent nodes rather of sending data drip the data. For the reason, that Sinkhole outbreak in the network is difficult to find out and thwart.

A. Necessity To Thwart Wormhole Outbreak

Wormhole attack can be without problems propelled in each type of transmitting protocols: on demand and proactive. The existence of two wormholes in the community can distract about 50% of the visitors via the cooperated nodes [14]. Wormhole attack fallouts in lessening of the performance of network and now and again they may additionally be in charge of breaking up the entire network. Henceforth there is the want to discover and thwart the wormhole attack.

IV. Proposed Wormhole Mitigation Technique

Trust model performs the computation, trust derivation, and application. Throughout trust computation, a linear combination technique estimates overall node trust consistent with trust factors and a negligible worth method to reckon a path's trust. Consistent with trust has following properties:

- Context Dependence: Trust relationships are applicable in an exceedingly specific context.
- Uncertainty: Trust depends on uncertainty of

nodes action. It offers action chance of a node.

- Quantitative value: Trust is assigned any numeric values; separate or continuous.
- Asymmetric Relationship: Trust relationship is uneven naturally. If node A trusts B and node B trust C that doesn't mean that A trusts C.

Trust of node j to a different node k could be a live guaranteeing that packets sent to node k by node j for forwarding were really forwarded by node k. Trust values from two trust factors (CFR and DFR) are assigned weights to see overall trust level for a selected node. Prompt trust in node k by node j is delineated as T_{jk} and given by following equation:

$$T_{jk}t_{(i)} = w1 * CFR_{jk}t_{(i)} + \ w2 * DFR_{jk}t_{(i)} \quad (1)$$

where $CFR_{jk}t_{(i)}$ and $DFR_{jk}t_{(i)}$ represent control packet forwarding ratio and data packet forwarding ratio observed by node j to forward node k at time t_i. Parameters w1 and w2 reflect weights assigned to CFR and DFR, respectively.

A distributed/adaptive applied mathematics identification technique to filter R_{REQs} (by destination) or R_{REPs} (by source) with excessive massive delays is planned. The bound is calculated on per hop R_{REQ}/R_{REP} packets time as completely different R_{REQs} take varied range of hops, that standard packets are preserved and falsified packets filtered. Retransmit timeout (RTO) calculations by protocol, that capture average and deviation of a connection's trip times are calculated.

A destination node filters R_{REQs} targeted to that during this style with overly giant delays. Contemplate a route discovery from supply S to destination D. D receives $R_{REQ's}$ first copy with hop count h1 at standard time t1, and second copy with hop count h2 at time t2.. Let t0 denote destination standard time once the request originated at supply. As actual worth of t0 is unknown, however D estimates it's seen below. First R_{REQ} with new sequence variety is taken into account legitimate and a destination sends a R_{REP} back to supply. For every duplicate R_{REQ} received, the destination calculates route request hop time (RHT), time for asking packet to succeed in destination divided by its hop count as shown in Equation (2).

Destination computes *RHT's* smoothed average, denoted *avgRHT*, and deviation, *devRHT*, for accepted R_{REQs}. To distinguish between malicious route requests and normal, a cut-off request hop time, *cutoffRHT* is calculated. For each duplicate R_{REQ} received, a corresponding reply is generated and avgRHT and cutoffRHT updated when this $R_{REQ's}$ *RHT* is below *cutoffRHT*. Destinations maintain separate *avgRHT* and *devRHT* values for all sources.

$$RHT_i = \frac{(t_i - t_0)}{h_i} \quad (2)$$

$$diff_i = (RHT_i - avgRHT) \quad (3)$$

$$avgRHT = avgRHT + \delta * diff_i \quad (4)$$

$$devRHT = devRHT + \mu * (|diff_i| - devRHT \quad (5)$$

$$cutoffRHT = avgRHT + \phi * devRHT \quad (6)$$

Various values were experimented with 0.5, 0.25 and 0.125 for μ and δ it is verified that 0.125 is best for both parameters.

The proposed architecture will be based on two-tier. In first-tier, local monitoring technique may be applied to detect and isolate malicious nodes locally based on the trust value. In the second tier, we develop a safe central authority for global tracing of node positions. When a strong suspicion builds at central authority in the second tier, it imposes a global separation of the malevolent node from the entire network. This mitigation problem will be analyzed through extensive simulation using network simulators by comparing with the existing standard approaches.

In our proposed methodology, we use two-tier authentication systems to separate the malevolent node from the network. In tier two, we consider the following conflictions as a necessary condition for the existence of wormhole in the network.

- A node is suspected to be malicious if RTT is larger than expected.
- If a particular node is assumed as a next hop neighbor by more than 'm' nodes. This confliction is considered by assuming that a wormhole node tries to attract more neighbors in its transmission radius.

This is accomplished by using Mamdani/ Sugeno Fuzzy inference technique by specifying four membership functions for RTT value. Low, medium, high and very high.

A. System Model and Assumptions

In our proposed technique we undertake symmetric, heterogeneous and mobile network. All community nodes' radio transceivers run under the equal configuration at some stage in the lifetime of the network. The unique identifier is assigned to every node. Our wormhole detection technique is centered on the RTT of the packet amongst nodes. Our challenge is that the opponent may additionally lengthen the RTT value amongst consecutive nodes.

When the nodes are deployed initially, the Wi-Fi starts the nearby discovery process. This gives a notion to every node in the community about with which sensor nodes it can speak directly. Then sensor nodes start off evolved facts transmission over an AODV routing protocol to send messages to their supposed receivers. For this precise application, it requirements the performance of the important routing protocol. Since nodes trade messages, the protocol has to provide nodes with routing important points so that nodes can send messages exactly to different nodes.

B. *Fuzzy Rules for the Proposed System*

Proposed two-tier wormhole attack mitigation is implemented using Mamdani/ Sugeno Fuzzy Inference System. Fuzzy If-Then rules are specified by 4 membership functions for RTT value. Low, medium, high and very high.

Rules are specified as shown in Table 1.

Table 1. Fuzzy Rules for Wormhole Mitigation

Rule	Antecedent 1	Antecedent 2	Consequence (Probability of existence of malicious nodes)
1	RTT-LOW	NN < m	0
		NN=m	LOW
		NN>m	HIGH
		NN>>m	HIGH
2	RTT-MEDIUM	NN < m	VERY LOW
		NN=m	VERY LOW
		NN>m	LOW
		NN>>m	HIGH
3	RTT-HIGH	NN < m	LOW
		NN=m	LOW
		NN>m	HIGH
		NN>>m	VERY HIGH
4	RTT-VERY HIGH	NN < m	LOW
		NN=m	LOW
		NN>m	HIGH
		NN>>m	VERY HIGH

Algorithm:

In this section, we propose a wormhole node mitigation algorithm. In Tier 1 if strong suspicion is generated, then Tier 2 is executed to authenticate the sensor nodes as explained below.

```
Wormhole Node Mitigation Algorithm
Tier 1:
    • Consider a set of nodes to be authenticated.
    • Generate the membership function for inputs RTT and number of neighbor nodes 'm' and assign output weight
    • Use Aggregation method for FIS to obtain the output.
    • Calculate the output weight using CoG technique.
    • Obtain the probability of the existence of the wormhole node in that area of network based on the fuzzy rules.
      Function Authentication(RTT, No. of neighbor nodes 'm')
Input: RTT and no. of neighbor nodes 'm' for a given sensor node in the given area.
Step 1: Begin
Step 2: Deploy sensor nodes in 500mx500m.
Step 3: Select a set of nodes.
Step 4: Initialize Authentication process at tier 1.
    • Membership functions are generated for input RTT, no. of neighbor nodes 'm' and output weight.
    • Generate the fuzzy rules (RTT, no of neighbor nodes 'm', probability)
    • Apply aggregation to FIS
    • Calculate the output weight as a probability from CoG.
Step 5: In tier 2, the nodes with a high probability of suspicion are eliminated.
Step 6: Update network topology.
Step 8: End.
```

V. Simulation and Experiment

Simulation set up is made in NS-2 Simulator and MATLAB for Fuzzy Inference System. Here we define the input membership function for RTT as low, medium, high and very high. Also the input membership function for the percentage of malicious nodes in the network. In MATLAB environment we obtain the probability of the existence of wormhole nodes in the network based on input membership functions RTT and percentage of Malicious/ Wormhole nodes.

A. *Results and Discussions*

Figure 4.1 shows the probability of wormhole attack existence for the membership functions RTT and the number of malicious nodes. When the Degree of membership for RTT> 1<2 hops and malicious nodes are 50%, then the probability of the existence of wormhole nodes are shown in fig. 4.1. When RTT is medium that is 3 hops, and malicious nodes introduced into the network is 50%, then the probability of the existence of wormhole in the network is depicted in fig. 4.2. When RTT is maximum that is 5 hops and malicious nodes in the network are 50%, then the probability of the existence of wormhole in the network is depicted in fig. 4.3. Figure 4.4 shows the surface view for the probability of the existence of wormhole nodes in the network.

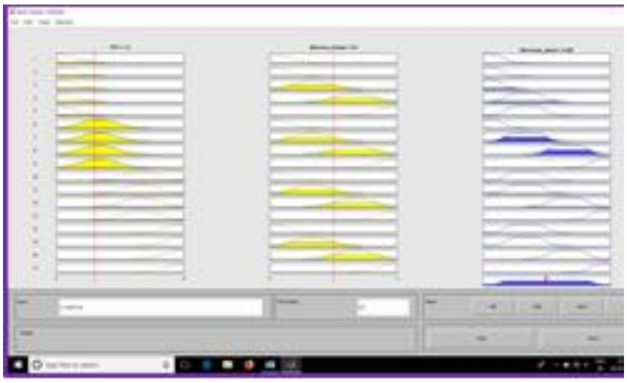

Fig.4. Degree of Membership for RTT= 1.5, Malicious Nodes=50%

From these graphs, we can conclude that if RTT is high and a number of malicious nodes present in the network are more then the probability of the existence of wormhole link is more. In tier 1 when the probability of suspicion built for the existence of wormhole exceeds the threshold value, then tier 2 is executed to remove the malicious nodes from the network and update the topology.

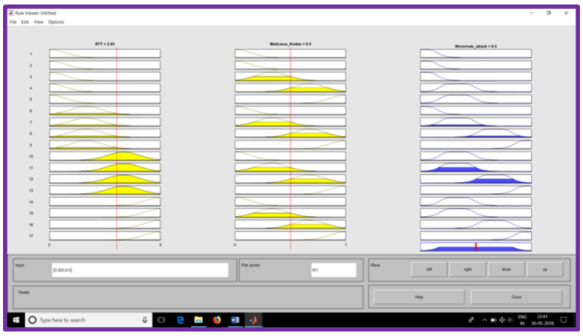

Fig.5. Degree of Membership for RTT= 3, Malicious Nodes=50%

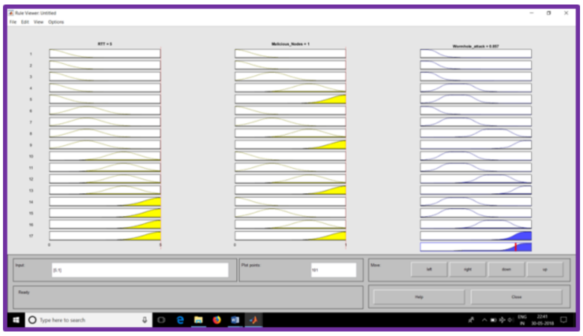

Fig.6. Degree of Membership for RTT= 5, Malicious Nodes=100%

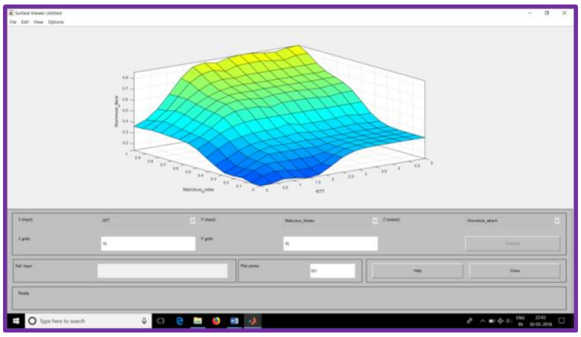

Fig.7. Surface view for Wormhole Existence in the Network

Sensor nodes (around 200) are deployed in the area of 500m x 500m.These nodes are assimilated with random waypoint mobility, AODV routing protocol in NS 2.34 Simulator. The simulation parameters are shown in Table 2.

Table 2. Simulation Parameters

Network size	500x500m
Number of nodes	450
Bandwidth	2 Mbps
Transmission range of node	250m
Transmission power of node	10mw
Antenna	Omnidirectional
Mobility model	Random way point
Power threshold	-95dB

The trial simulation outcomes for PDR are presented in Table 3.

Table 3. No. of Nodes v/s PDR

No. of Nodes	PDR of proposed system (in %)	PDR of scheme1 (in %)	PDR of scheme2 (in %)
100	80	76	80
150	95	94	92
200	100	95	94

Figure. 8 shows Packet delivery ratio for proposed detection system, scheme 1 and scheme 2. PDR for proposed system is better than 3% as that of scheme 1 and 3.3% better than that of scheme 2.

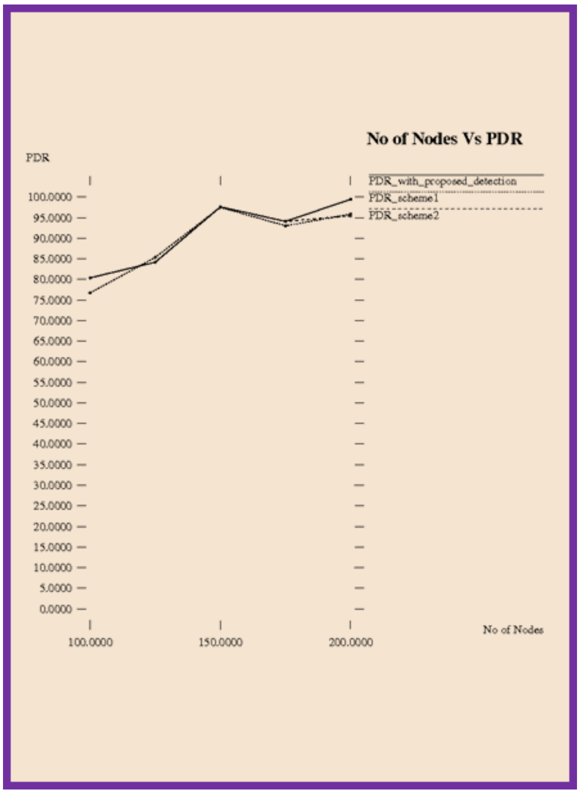

Fig.8. Packet Delivery Ratio

The trial simulation outcomes for PDR are presented in Table 4.

Table 4. No. of Nodes v/s Throughput

No. of Nodes	Throughput of proposed system (in Kbps)	Throughput of scheme1 (in Kbps)	Throughput of scheme2 (in Kbps)
10	100	100	100
20	380	355	350
30	360	358	355
40	50	50	50

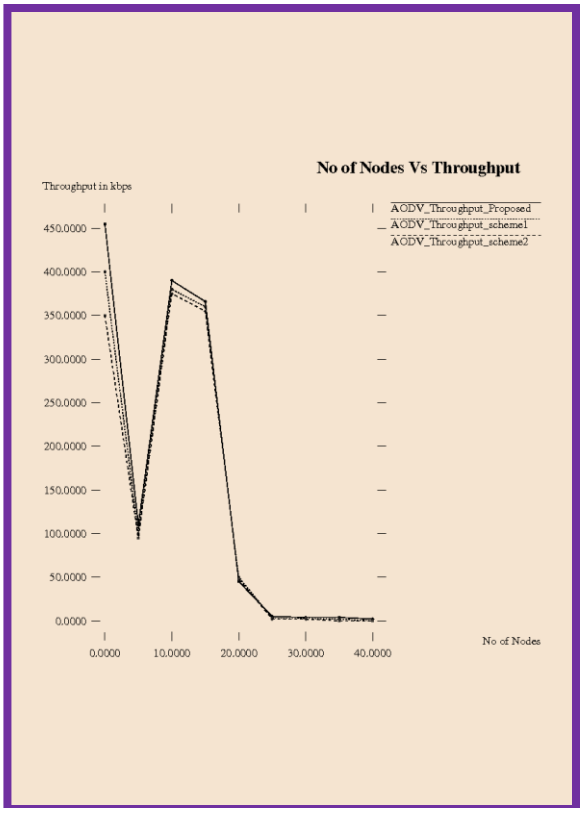

Fig.9. No. of Nodes v/s Throughput

Figure. 9 shows the comparison of AODV throughput for proposed system, scheme 1 and scheme 2. AODV routing protocol's performance is better in our proposed system is better by 0.0168% compared to scheme 1 and 0.0218% better than that of scheme 2.

VI. Conclusions

In this paper, we have described the two-tier distributed wormhole mitigation technique using Mamdani/ Sugeno FIS. Here we define 4 membership functions as Low, Medium, High and Very high are specified. Output variable includes 5 membership function (Very High, High, Medium, Low, and Very Low). Very High defines the high probability of the existence of wormhole node in the network. We use the most common fuzzy inference techniques. In Fuzzification, fixed values of the input received for input variables and are determined that the inputs are assigned to each fuzzy set. And in Evaluation rules, fuzzy input values are received. Min method is used at this stage. Output rules, output all the rules. In this stage, the MAX method is used. In Defuzzification, input to this process, the aggregate output fuzzy set, priority, and its output is a constant value. The domain value corresponding to rule is the number of rules triggered in the fuzzy inference engine and the predicate truth for that domain value.

References

[1] P. B. Hari and S. N. Singh, "Security issues in Wireless Sensor Networks: Current research and challenges," 2016 Int. Conf. Adv. Comput. Commun. Autom., pp. 1–6, 2016.

[2] P. Tague and R. Poovendran, "Modeling Node Capture Attacks in Wireless Sensor Networks Invited Paper," Electr. Eng., pp. 1221–1224, 2008.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Proc. First IEEE Int. Work. Sens. Netw. Protoc. Appl. 2003., pp. 113–127, 2003.

[4] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks, ICSNC'06: Proceedings of the International Conference on Systems and Networks Communication, Washington, DC, USA, IEEE Computer Society, 2006, 40.

[5] J. Rehana, "Security of Wireless Sensor Network," p. 10, 2009.

[6] J. Walters and Z. Liang, "Wireless sensor network security: A survey," Secur. Distrib. …, pp. 1–50, 2007.

[7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[8] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, 2010.

[9] J. A. Chaudhry, U. Tariq, M. A. Amin, and R. G. Rittenhouse, "Dealing with Sinkhole Attacks in Wireless Sensor Networks," ASTL Sectech, vol. 29, no. SecTech, pp. 7–12, 2013.

[10] Majid Meghdadi, Suat Ozdemir, and Inan Güler, ―A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks,‖ IETE technical review, VOL 28, ISSUE 2, 2011.

[11] P. Niranjan, M. Shrivastava, and R. Singh Khainwar, "Enhancement of Routes Performance in MANET Avoiding Tunneling Attack," Int. J. Comput. Appl., vol. 42, no. 12, pp. 28–32, 2012.

[12] S. Ji, T. Chen, S. Zhong, and S. Kak, "DAWN: Defending against wormhole attacks in wireless network coding systems," INFOCOM, 2014 Proc. IEEE, pp. 664–672, 2014.

[13] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1787–1796, 2011.

[14] Z. T. and A. H. Maw., "Wormhole attack detection in wireless sensor networks," Proc. World Acad. Sci. Eng. Technol. Technol., vol. 46, no. 3, pp. 545–50, 2008.

[15] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE INFOCOM 2003. Twenty-second Annu. Jt. Conf. IEEE Comput. Commun. Soc. (IEEE Cat. No.03CH37428), vol. 3, pp. 1976–1986, 2002.

[16] Z. Zhao, B. Wei, X. Dong, L. Yao, and F. Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," 2010 WASE Int. Conf. Inf. Eng., pp. 251–254, 2010.

[17] W. Wang and B. Bhargava, "Visualization of wormholes

in sensor networks," Proc. 2004 ACM Work. Wirel. Secur. - WiSe '04, p. 51, 2004.

[18] I. Khalil, S. Bagchi, and N. B. Shroff, "LITE WORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks," Proc. Int. Conf. Dependable Syst. Networks, no. August 2015, pp. 612–621, 2005.

[19] R. Z. El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy, "DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks," no. August 2014, 2005.

[20] L. Buttyán, L. Dóra, and I. Vajda, "Statistical Wormhole Detection in Sensor Networks," Secur. Priv. Ad-hoc Sens. Networks, pp. 128–141, 2005.

[21] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "TrueLink: A practical countermeasure to the wormhole attack in wireless networks," Proc. - Int. Conf. Netw. Protoc. ICNP, pp. 75–84, 2006.

[22] R. Poovendran and L. Lazos, "A graph-theoretic framework for preventing the wormhole attack in wireless ad hoc networks," Wirel. Networks, vol. 13, no. 1, pp. 27–59, 2007.

[23] S. Madria and J. Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks," Ad Hoc Networks, vol. 7, no. 6, pp. 1051–1063, 2009.

[24] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Chapter 14 DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS."

[25] T. Hayajneh, P. Krishnamurthy, and D. Tipper, "DeWorm: A simple protocol to detect wormhole attacks in wireless ad hoc networks," NSS 2009 - Netw. Syst. Secur., pp. 73–80, 2009.

[26] Z. Zhao, B. Wei, X. Dong, L. Yao, and F. Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," 2010 WASE Int. Conf. Inf. Eng., pp. 251–254, 2010.

[27] S. Gupta, S. Kar, and S. Dharmaraja, "WHOP: Wormhole attack detection protocol using hound packet," 2011 Int. Conf. Innov. Inf. Technol. IIT 2011, pp. 226–231, 2011.

[28] S. K. Dhurandher and I. Woungang, "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks," 26th Int. Conf. Adv. Inf. Netw. Appl. Work., pp. 472–477, 2012.

[29] A. Louazani, L. Sekhri, and B. Kechar, "A time Petri net model for wormhole attack detection in wireless sensor networks," 2013 Int. Conf. Smart Commun. Netw. Technol., pp. 1–6, 2013.

[30] B. Tian, Q. Li, Y. X. Yang, D. Li, and Y. Xin, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," J. China Univ. Posts Telecommun., vol. 19, no. SUPPL. 1, pp. 6–10, 2012.

[31] H. M. Choi, S. M. Nam, and T. H. Cho, "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks *," vol. 2013, no. March, pp. 33–40, 2013.

[32] G. Wu, X. Chen, L. Yao, Y. Lee, and K. Yim, "An efficient wormhole attack detection method in wireless sensor networks," Comput. Sci. Inf. Syst., vol. 11, no. 3, pp. 1127–1142, 2014.

[33] N. Agrawal and N. Mishra, "RTT based wormhole detection using NS-3," Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014, pp. 861–866, 2014.

[34] J. H. Zheng, H. Y. Qian, and L. Wang, "Defense technology of wormhole attacks based on node connectivity," Proc. - 2015 IEEE Int. Conf. Smart City, SmartCity 2015, Held Jointly with 8th IEEE Int. Conf. Soc. Comput. Networking, Soc. 2015, 5th IEEE Int. Conf. Sustain. Comput. Communic, pp. 421–425, 2015.

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

[36] D. S. Bhatti, S. Saeed, M. A. Ullah, N. S. Naaz, S. S. R. Rizvi, and S. T. Ali, "SRoWM: Smart Review on Wormhole Mitigation," Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 12, pp. 178–187, 2017.

Authors' Profiles

Sharada Kori, Research Scholar in Visvesvaraya Technological University, Karnataka India.

Her main research interests include wireless sensor networks and Embedded Systems.

Dr. Krishnamurthy G. N, Research Supervisor, VTU, Belagavi, Principal, BNM Institute of Technology, Bangalore, Karnataka, India. His main research interests include distributed computing, wireless networks, data analytics, machine learning and artificial intelligence. He has published his papers in various journals/conferences at international level where the proceedings are published in various indexing services like IEEE Xplore, DBLP, etc. Some of his research works are published in various international journals such as International Journal of Computer Science and Network Security and International Journal of Network Security and Applications.

His areas of interest include cryptography, distributed computing, wireless networks, data analytics, machine learning and artificial intelligence.

He is a member of the Indian Society for Technical Education (ISTE) and International Association of Engineers

Dr. Nandini Sidnal, Professor and Research Supervisor in VTU, Belagavi, Karnataka, India. Her main research interests include distributed computing, E-commerce, E-learning, wireless networks, agent technology, parallel computing and cloud computing. She is a member of the Indian Society for Technical Education (ISTE), associate member of Agent Link, member of IEEE and member of ACM.

How to cite this paper: Sharada Kori, Krishnamurthy G N, Nandini Sidnal,"Distributed Wormhole Attack Mitigation Technique in WSNs", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.5, pp.20-27, 2019.DOI: 10.5815/ijcnis.2019.05.03