International Journal of Computer Engineering & Technology (IJCET)
Volume 9, Issue 3, May-June 2018, pp. 148–158, Article ID: IJCET_09_03_017
Available online at
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=3
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

INTEGRATED APPROACH TO DEFEND JAMMING ATTACK IN WSN

Annu Joshi
Research Scholar, Banasthali Vidyapith,
Tonk Distt., Rajasthan, India

Anup Bhola
Assistant Professor, Banasthali Vidyapith,
Tonk Distt., Rajasthan, India

G.N. Purohit
Professor, Banasthali Vidyapith,
Tonk Distt., Rajasthan, India

ABSTRACT

WSN is first choice of mission-critical applications such as navigation system, military, monitoring, industrial application and health sectors also. Larger demand makes it more prone to malicious attacks. Jamming attack is one of the malicious attacks which occupy the sensor by emitting larger bandwidth frequency. Thus jamming attack can manipulate the sensor according to its poisonous will i.e. to delay message broadcast in emergency situation and also degrade the throughput of WSN. In mission-critical situation message broadcast is must to avoid accident, e.g. navigation system and message alert situation. In order to disseminate the message efficiently, spread spectrum technique can be used because it can handle powerful jammer. Drawback of using it is that there is wastage of crucial bandwidth because to data it uses vast frequency band as compared to sending data frequency. To compensate this drawback, we merge mobile agent(MA) technique to spread spectrum(SS) technique to efficiently save the energy.MA technique by comparing assigned threshold value to nodes, can detect the jammed node and send alert message to base station and then base station accordingly take the action.

In this paper, we will evaluate the merits and demerits using this integrated approach with SS and MA technique.

Key words: WSN, Jamming Attack, mobile agent(MA), spread spectrum(SS).

Cite this Article: Annu Joshi, Anup Bhola and G.N. Purohit, Integrated Approach to Defend Jamming Attack in WSN. *International Journal of Computer Engineering and Technology,* 9(3), 2018, pp. 148-158.
http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=9&IType=3

1. INTRODUCTION

WSN's attractive feature is its mobility. Many applications are enticed by this charming property of WSN. Some applications are general purpose and others are mission-critical. Transportation, healthcare. Industrial and military applications come under mission-critical applications. In mission-critical environment, systems are usually built upon WSN that need to provide timely and valid info about the field, e.g. GINSENG project is a European project where main objective is to achieve a performance controlled WSN to provide reliable operation in critical scenario such as in oil refineries. To check health status of refinery personnel in hazardous environment. This can be done by WSN and employees can be monitored in real time equipping their suits. Sensor mobility has its own issues such that routing activity, monitoring of sensors deployed and security threats. There are many protocols working behind WSN to tackle these challenges. Jamming attack is one of those challenges. Spread Spectrum technique is one technique that comes in mind first when we think about how to handle jamming attack in WSN. These techniques share pair wise secret keys between sender and receiver before communication. Frequency hopping spread spectrum (fhss) and direct sequence spread spectrum (dsss) are important SS techniques. Sender and receiver share secret key before communication, and enable receiver to generate the random sequence and decode the sender's spread signal. This benefit has its own pitfalls, one of which is bandwidth wastage. Mobile agent technology can prove itself as a savior for this deficiency of spread spectrum technique. By combining these two hardware based and software based technology, we can enhance the total throughput of WSN In this paper, we would evaluate our integrated approach with Mobile agent technique with SS modulation in mission critical situation.

2. RELATED WORK

Wireless communication jammers have been widely analyzed and categorized in terms of their capabilities (e.g., broadband or narrowband) and behavior (e.g., constant, random, responsive, sweep) by Poisel et al[1], Xu et al [2], Li et al[3]. Many jammer models used in prior works Poisel et al [1],[Xu et al,Li et al,Aaalj et al, [2]–[4] cover the interference with transmissions in terms of signal jamming as well as dummy packet/preamble insertions[22]. In [5]Chiang et al, [6] Desmedt et al, the respective authors address broadcast jamming mitigation based on spread-spectrum (SS) communication. Common to these broadcast schemes as well as to other proposed countermeasures against denial-of-service attacks in wireless networks [2], [4], [5]–[7]Noubir et al, is that they all rely *on secret keys, shared between the sender and* receiver(s) prior to their communication. However, pre-establishing keys between devices in ad-hoc networks for subsequent SS communication suffers from scalability and network dynamics problems. Key-establishment approaches that rely on device proximity [8]–[12][Stajano et al,Mccune et al,Goodrich et al,Apkun et al,Gehrmann et al] can be used in this context, but require the nodes to be physically close to each other and to use communication channels that are not being jammed (e.g., infrared, wire, or visual). The requirement of pre-shared secrets (keys) at the expense of a reduced communication throughput. According to[21],there is significant amount of work is done on algorithmic approach to detect jamming attack also. Wood et al [13], mapping protocol for nodes that surround a jammer is proposed. Using this approach, the protocol creates awareness in the neighboring nodes to detect a jamming attack using message diffusion. Also, in this paper single-channel wireless communication is assumed. It is simulated using GloMoSim simulator with different range of jammingattack and neighboring nodes. The protocol was robust (message re-routed and only loses data in inactive nodes) to failurerates of 20-25% of mapping nodes from twelve neighboring nodes within communication range.In [14]

Newsome et al tells us about sybil attack on a network and routing layer of WSN is analyzed. Here it is assumed that a sensor node communicates with its neighbors using half-duplex and single radio with various channels. The process of identifying sybil attacks is based on radio resource testing. Legitimate neighboSring nodes are allotted a single channel for identity. This process of identifying a sybil attack cannot function if the spectrum is jammed. Hence, would lead to a false identification of a sybil attack. In [15]Karlof et al tells about routing security in sensor network is analyzed and a countermeasure is proposed. Defense mechanism for different DoS attacks such as spoofing, wormhole, sybil, selective forwarding etc., is given based on the assumption that using radio frequencies alterations can be made to the data. Radio jamming using traditional methods in military environments is summarized in this paper. Muraleedharan et al[16] talks about cross layer DoS attack using detection usins Swarm Intelligence. In [17] Silva et al while working on a European project GINSENG, propose a scheme which enables mobility in network in critical applications. In [18], Mpitziopoulos et al describe open research issue in wireless sensor network and defense strategies to combat them. C. Popper et al in [19] proposed a scheme using un- coordinated spread spectrum techniques to cobat jamming attack in wireless sensor network. Joshi et al in [20] proposed a scheme which is a merger of two techniques spread spectrum and mobile agent technique to combat jamming attack efficiently. Our contribution in this paper is that we are proposing an algorithm which is a integration of spread spectrum technique and mobile agent technique and evaluate its performance in real world scenario whether it is compatible or not.

3. PROBLEM DESCRIPTION

Jamming is defined as act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. This attack interferes with the radio frequencies and then manipulating them further. These signals are white noise or any signal resembling network traffic. For a successful jamming signal to noise (SNR) ratio should be less than 1, where SNR=P (signal)/P(noise),where P is power.

Jamming attack is more pronounced at physical and MAC layer due to their resource allocation nature. Jamming attack affects the QoS of resource constrained sensors. There are different types of jamming types:

1. Spot Jamming: It is vastly used jamming method which uses all its transmitting power on a single frequency that the target uses with the same modulation. It can easily overpower the original signal. It can be avoided by changing frequency to another frequency.

2. Sweep Jamming: In this type, jammer's full power changes itself from one frequency to another. It can jam multiple frequencies in quick successions but does not jam them all at the same time. It can cause considerable packet loss.

3. Barrage Jamming: This type can jam multiple frequencies at same time. Its effectiveness decreases with increasing jamming frequencies.

4. Deceptive Jamming: It is most dangerous jamming technique in which adversary doesn't want to disclose her identity. It can jam a single frequency and multiple frequencies as well.

Types of Jammer

Constant Jammer: This type of jammer continuously emits random radio frequency without following any MAC protocols to make channel busy.

Deceptive Jammer: By hiding its own identity, adversary manipulates the network.

Reactive Jammer: It sees activity and then immediately sends out a random signal to collide with the existing signal on the channel.

Random Jammer: This type of jammer is not fully functional in the network. It randomly manipulates the network without any sequence.

Counter Measures

1. Proactive Techniques: This type of countermeasure is to make a WSN immune to jamming attack rather than reactively respond to such incidents. They can be implemented as algorithmic way or with special hardware equipped with algorithms,e.g. DEEJAM algo.

2. Reactive Techniques: This technique enables reaction only when it senses jamming attack in WSN, e.g. JAM algo.

3. Detection Techniques: This technique instantly detect jamming attack but it needs other countermeasures along with to efficiently do its job.

4. Mobile Agent Based Techniques: MA based system is an autonomous program which works on behalf of users. They are called data aggregators e.g. JAID algo and ANT system.

Detection techniques are less efficient due to extra hardware and thus needs extra energy .Proactive is algorithmic based approach but inefficient in case there is more powerful jammer than DEEJAM. With hardware, it is expensive. It is good for constant, random and deceptive jamming. In reactive techniques, JAM can't jam when all nodes are jammed or significant amount of nodes are jammed. This technique is good for reactive jamming.MA based techniques lack an optimal hardware associated with it which could defend WSN in case of powerful jammer.

The approach adopted by us in this paper is a combined approach of spread spectrum technique and mobile agent technique. Spread Spectrum technique has disadvantage that it use much more bandwidth than requirement to transmit data. But SNR and interferences decreases significantly by using spread spectrum technique(FHSS).On the other hand, MA technique has upper hand to detect suspicious sensors and malicious node and in this way to make that sensor out of WSN and decide another path to communicate. But its main drawback is that it can't handle jammer with higher frequency or can say can't handle powerful jammer. So, by merging these two techniques, their drawbacks are compensated by each other. The crucial bandwidth of SS is saved by applying MA filter which detect the malicious node and The inefficiency of MA to handle powerful jammer is compensated by applying Spread spectrum technique .

4. INFORMAL EXPLANATION OF PROCEDURE

Ours integrated approach works on two techniques in parallel. It is just like coming together the best of the two worlds. Powerful modulation technique first overrides the interferences and if there any type of jamming happening in network then MA would detect that and accordingly alert the BS(base station) and BS would take action accordingly.

So, by combining efficient hardware which would provide effective defense with efficient algorithmic measure, we can enhance the overall throughput of WSN.

Procedure Data Base Used

Mobile Agent Table: It consists of three parameters namely sensor id assigned by BS, node authentication method via polynomial function and threshold value assigned to that particular node id.

Base Table: It consists of node ids of jammed nodes which can be modified or reinstructed during the communication across the network.

In this integrated scheme, powerful security server attached with base station assigns each node a unique _id which is saved in both Base Table and Mobile Agent Table. .Security server also provides each sensor node a unique verification polynomial which is based on a one way hash function h(.) that could be MD5,SHA etc. .

In this scheme, we consider the communication medium via frequency hopping spread spectrum technique which is co-ordinated i.e. sender and receiver would share some secret key before communication takes place. This type of communication is based on a unique seed value assigned to the node generated by the base station through RandAlgo. This algorithm is used for generating pseudo random numbers. There is a frequency pool among which sender chooses its desired frequency to send messages. The receiver knows about the allotted frequency pool by knowing seed value. In this way, communication takes place. The BS frequently switches its frequency channels to avoid reactive jamming attack. The messages are divided into smaller fragments and are encoded by hash function h(.).Mobile agents traverse the whole network. Its main work is to calculate unique polynomial function on behalf of sensor node. In this way, it unburdens the sensor nodes from extra task of calculations. Here, in this way, MA verifies static entities allotted to sensor nodes. Further, energy exhaustion at abnormal way signifies a malicious attack. Here, packet delievery ratio which is proportional to energy exhaust by a particular node taken as dynamic identity to verify a node.MA decides an optimal packet delivery ratio as threshold value to detect any malicious activity. So, MA identifies both static entities as well as dynamic entities.

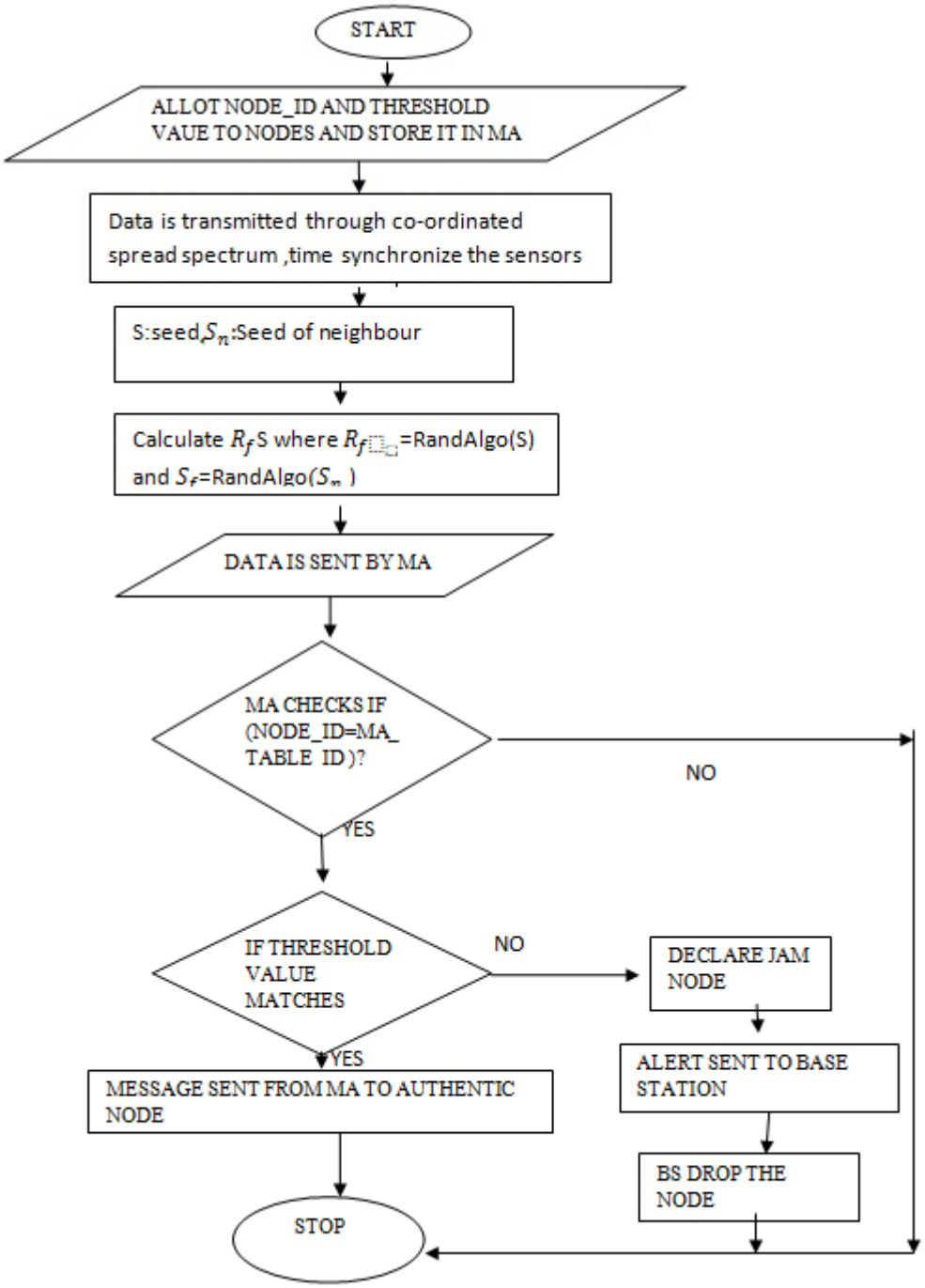
At each round of communication, MA first mathches the static identities of node and then threshold value, and if the identities are according to data stored in MATable then further communication takes place.

Flow chart and Psuedocode for the Scheme suggested

Psuedocode for Procedure

```
Set node_id=n(n1,n2,……..)
Set Seed value S
Threshold_value=n_th(n_th1,n_th2,…….),store in ma_table.
Mobile _agent(n.n_th)
{
 Calculate R_f S where                    seed of sending node is to be calculated //$
R_f=RandAlgo(S) and S_f=RandAlgo(S_n)

   If (n=n')                    //n' is node id stored in ma table.
   {
      If(Threshold value=n_th value)       //n_th value is stored in ma_table
    {
       Message is sent to authentic node
    }
  Else
        {
      Declare jammed node.
      Send message to base station.
      Base station drop the node.
   }
}}
}}
```



5. SIMULATION

This proposed integrated scheme is implemented in MATLAB 2013 Simulator. The performance of the algorithm is evaluated on the basis of throughput of the network and packet delivery ratio before and after the attack. In this experiment, no. of nodes which are deployed in sensor network are 100 and for the sake of stability of mechanism,1000 hops are taken for consideration before evaluating the result.At each hop,the remaining energy left in each node and the distance between node and base station would decide the future of that particular node whether it would take part in further iterations.

Simulation Results

In this experiment we are taking 100 nodes in a 120mX 100m area. Fig 1. Shows the network deployment and Fig. 2 represents the network with malicious jammers. Base station distributes each node an unique id and threshold value. When data is processed in this mechanism, Mobile agent checks the node id and predefined threshold value to detect any jamming attack in network.

The main parameter to determine threshold value is packet delivery ratio. Fig. 3 and fig 4. Represent the network throughput with integrated approach and comparative evaluation of this technique with or without jamming attack detection. Fig. 5 and fig. 6 represent packet delivery ratio with integrated approach and compative evaluation with or without jamming attack detection in network. Major performance enhacement is being seen by detecting jamming attack in network. Fig 7 is a table generation for this algorithm which shows this algorithm effectiveness and efficiency to deliver messages in jamming infested area.

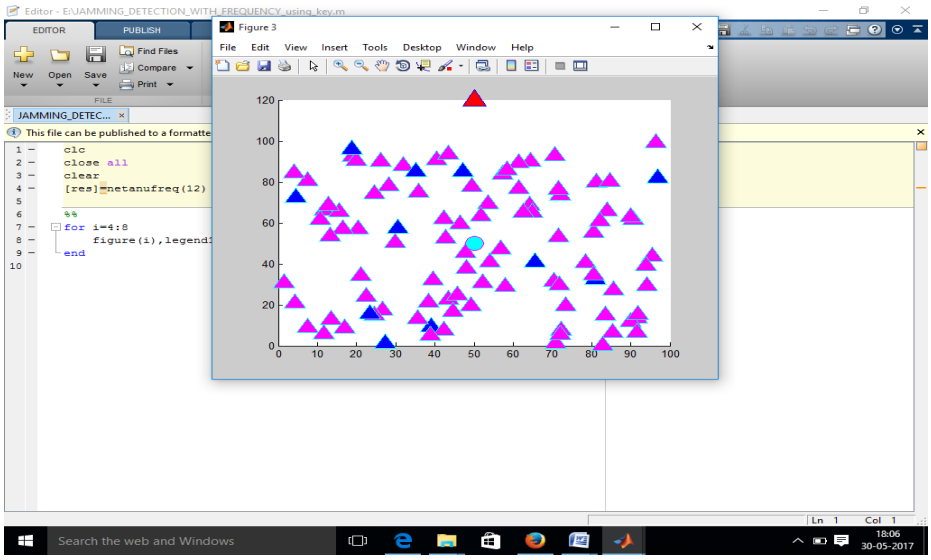


Figure 1 Network Deployment with nodes and jammer nodes(Red node(Base Station),Sky Blue circle(Mobile Agent),Pink node(nodes with ids and blue node as jammer nodes)

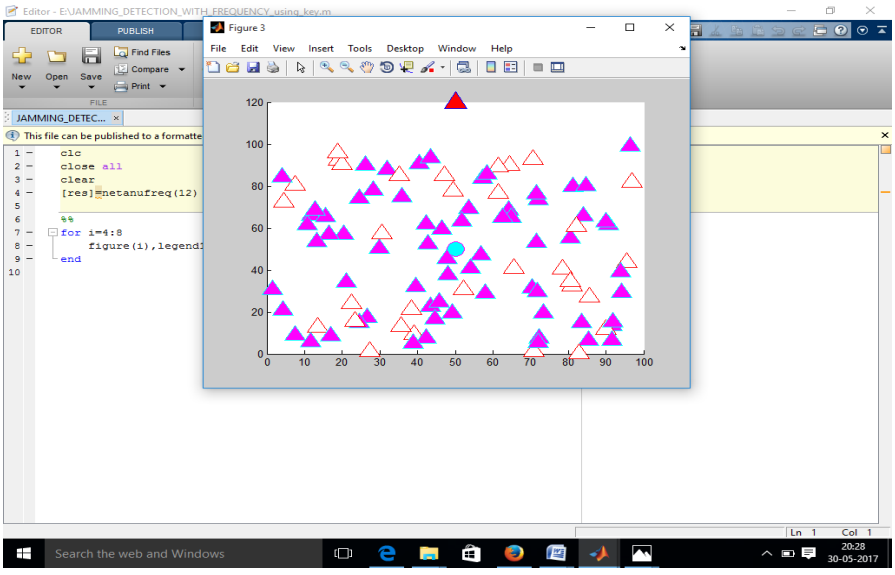


Figure 2 Jamming Detection by Mobile agent(hollow nodes indicate jammer nodes which are now disabled)

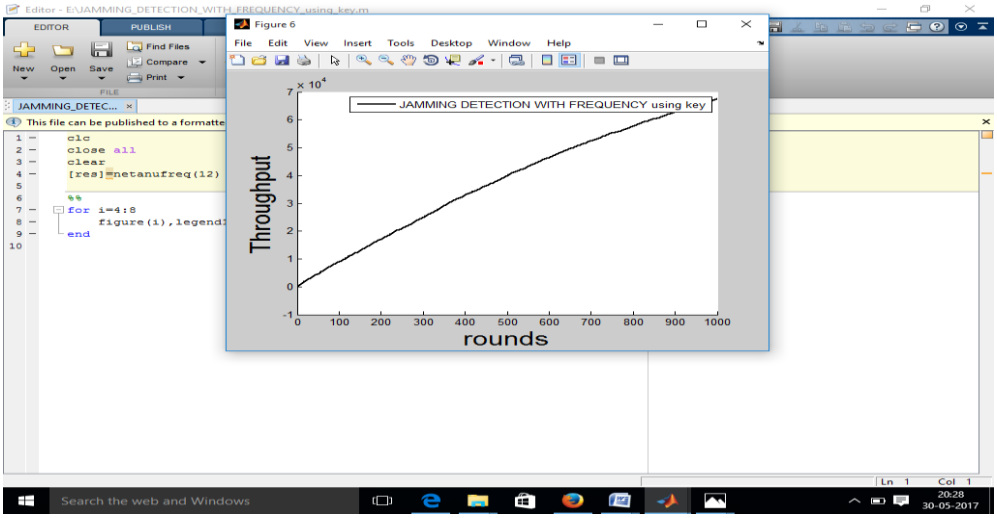


Figure 3 Throughput of network with integrated scheme

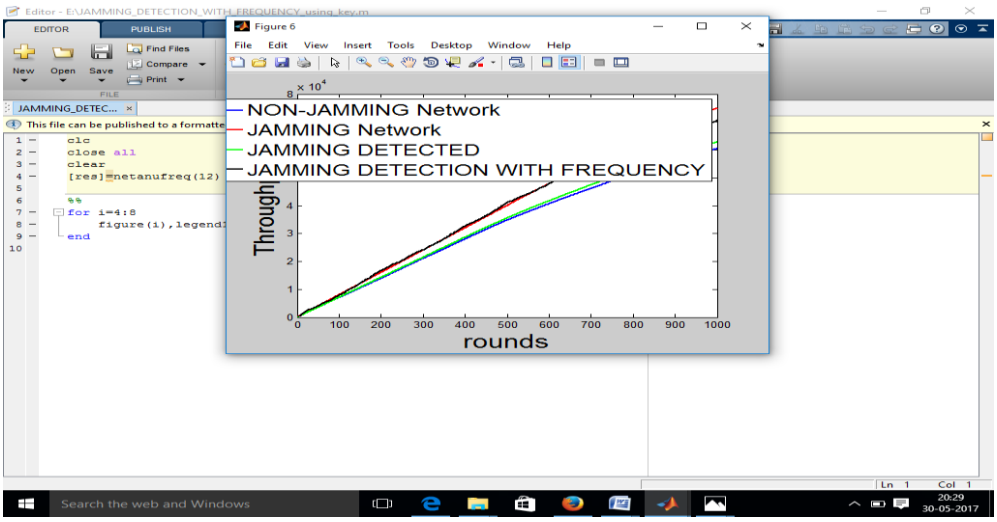


Figure 4 Comparative throughput of network with jamming and with jamming detection using integrated approach

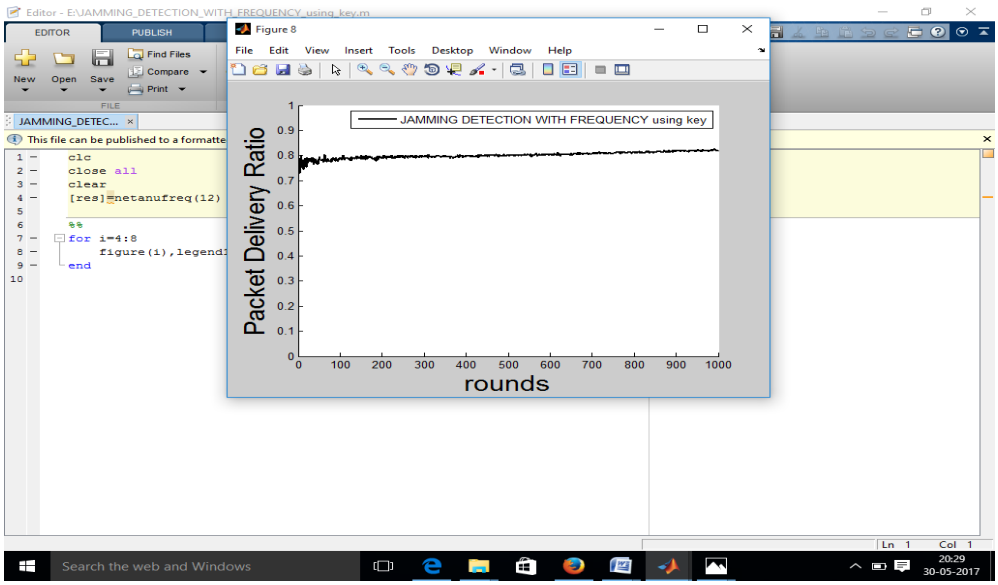


Figure 5 Packet delivery ratio using integrated scheme

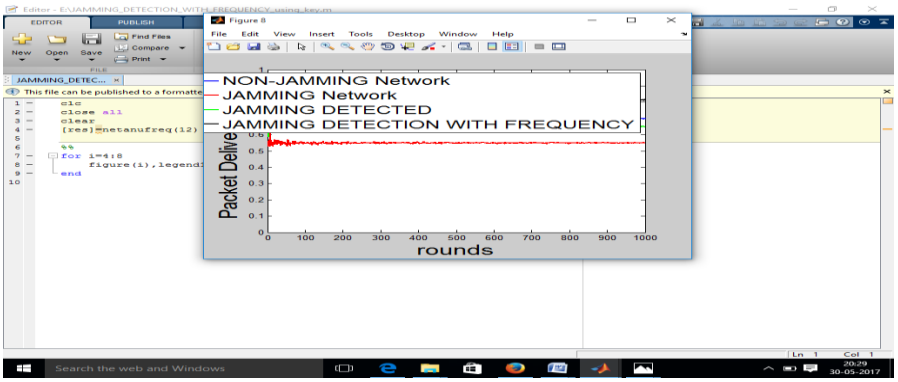


Figure 6 Comparative packet delivery ratio with jamming and with jamming detection by using integrated approach

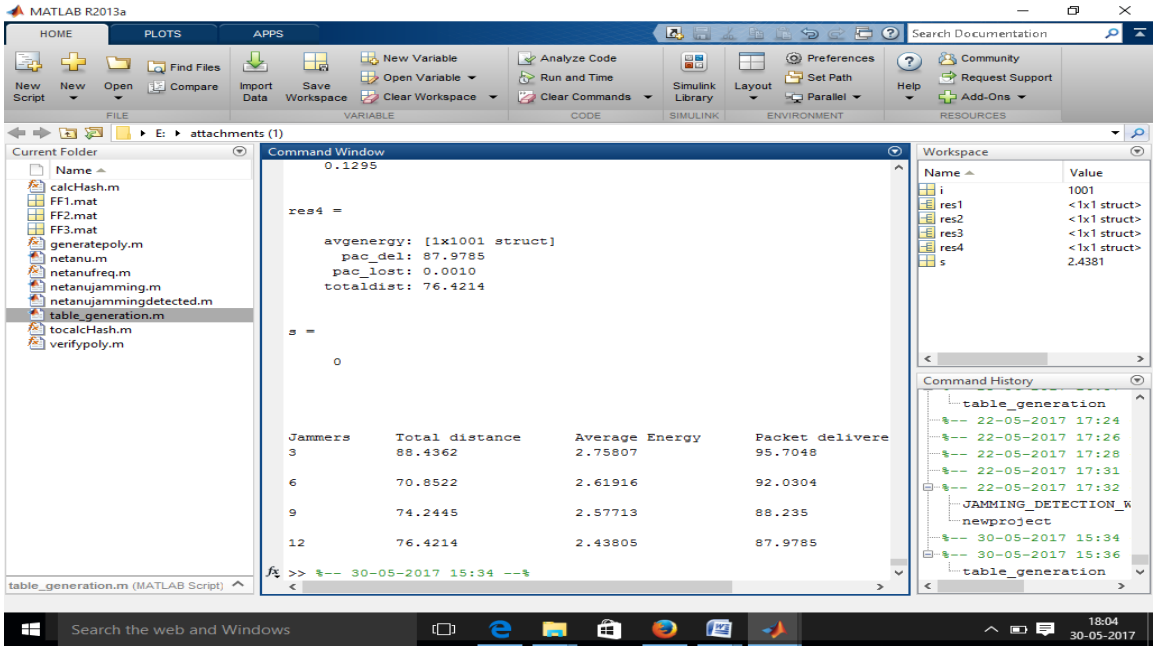


Figure 7 Table showing effectiveness of this integrated approach in WSN

6. CONCLUSION AND FUTURE WORK

Jamming attack is a great security threat for the efficient working of sensor network. The previously suggested schemes either do compromise on cost level or on security level. Ours proposed scheme takes into account both the factors i.e. cost and security simultaneously. In future, we would compare this integrated scheme to the merger of un-coordinated spread spectrum techniques and mobile agent technique. By comparing these two schemes, we would find out the ground reality to implement these techniques in real world scenario.

REFERENCES

[1] R. A. Poisel, Modern Communications Jamming Principles and Techniques. Artech House Publishers, 2006.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[3] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in Proceedings of the IEEE International Conference on Computer Communications(Infocom), 2007.

[4] M. Cˇ agalj, S. Cˇ apkun, and J.-P. Hubaux, "Wormhole-based antijamming techniques in sensor networks," IEEE Transactions on Mobile Computing, vol. 6, no. 1, pp. 100–114, 2007

[5] J. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in Proceedings of the IEEE International Conference on Computer Communications (Infocom), 2008.

[6] Y. Desmedt, R. Safavi-Naini, H. Wang, C. Charnes, and J. Pieprzyk, "Broadcast anti-jamming systems," in Proceedings of the IEEE International Conference on Networks (ICON), p. 349, 1999.

[7] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mobile Computing and Communications Review, vol. 7, no. 3, pp. 29–30, 2003.

[8] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Proceedings of the 7th International Workshop on Security Protocols, Springer-Verlag, 2000.

[9] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in Proceedings of the IEEE Symposium on Security and Privacy, 2005.

[10] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and clear: Human-verifiable authentication based on audio," in Proceedings of the IEEE International Conference on Distributed Computing Systems, 2006.

[11] S. Cˇ apkun and M. Cˇ agalj, "Integrity regions: authentication through presence in wireless networks," in Proceedings of the 5th ACM workshop on Wireless Security (WiSe), 2006

[12] C. Gehrmann, C. J. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, no. 1, 2004

[13] A. D. Wood,J. A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", Proceedings of the 24th IEEE International Real-Time Systems Symposium.2003.

[14] J. Newsome, E.Shi,D. Song and A.Perrig,"The Sybil Attack in Sensors Networks: Analysis and Defenses",Issue 27,April 2004(IPSN).

[15] C.Karlof and D. Wagner, "Secure routing in Wireless Sensor Networks: Attacks and Countermeasures", In First IEEE International Workshop on Sensor Network Protocols and Applications,2003.

[16] R.Muraleedharan and L.A.Osadciw,"Jamming Attack Detection and Countermeasures In Wireless sensor Network Using Ant System", IEEE Upstate New York Networking Workshop, Syracuse University, Syracuse NY,October,2003.

[17] R.Silva,Z. Zinonos, J.S.Silva and V.Vassiliou,"Mobility in WSN for Critical Applications", IEEE Symposium on Computers and Communications(ISCC),2011.

[18] A.Mpitziopoulos, D.Gavalas, C.Konstantopoulos and G.Pantziou,"Jamming in Wireless Sensor Networks", I EEE Communication Survey and Tutorials Conference,2009.

[19] C.Popper, M.Strasser and S.Capkun,"Anti-jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 5, JUNE 2010

[20] A.Joshi and G.N. Purohit," A Novel Approach to Hinder Jamming Attack In WSN", Communication on Applied Electronics,1(2),9-13,2015.

[21] URL: www.cognitiveintelligence.com

[22] URL: www.syssec.ethz.ch