International Journal of Systems Signal Control and Engineering Application

MEDWELL PUBLICATIONS

Packet Classification Methods over Jamming Attacks

[1]Pavan Kumar Kolluru, [2]K. Sri Vijaya and [2]M.E.K.A. Sowjanya
[1]*Department of Computer Science and Engineering, Vignan University, Vadlamudi, 522213 Andhra Pradesh, India*
[2]*Department of Information Technology, PVPSIT, Vijayawada*, India

Key words: Jamming attacks, RREP, RERR, RREQ, widely attacking

Corresponding Author:
Pavan Kumar Kolluru
Department of Computer Science and Engineering, Vignan University, Vadlamudi, 522213 Andhra Pradesh, India

Page No.: 148-151
Volume: 12, Issue 6, 2019
ISSN: 1997-5422
International Journal of Systems Signal Control and Engineering Application

Abstract: Wireless ad hoc network having the increasing feature due to their mobility, dynamic nature, easy to deployment. Jamming attacks are the most widely attacking models in wireless networks. In wireless networks the data transfer from source to destination is very important. Though there are no of nodes in the wireless networks there should be the source and destination should be defined. Various researches have been done on wireless networks to solve the jamming problems. In this study the jamming problem addressed in packet classification jamming traditionally used reactive protocols are RREP, RERR, RREQ, RREP are used for primary message format with adversary selective targets in launching of jamming attacks. The proposed system focus on detecting the jamming attacks and makes the route clear for data transfer within the wireless network. Results show the performance of proposed system.

INTRODUCTION

Data transfer should be done from source to destination in wireless networks. Without losing the data in the network when the data transferring it is possible in wireless network only with the related protocols implemented (Benyamina *et al*., 2012). In this wireless sensor networks, wireless networks is a self configurable networks. In mobile ad hoc network every node randomly moving into appropriate direction from base station other nodes present in network.

As shown in Fig. 1 nodes can be moved efficiently and dynamically into other nodes present in wireless networks. In this process of network communication jamming is the problem for decreasing network performance with emergency requirement present in wireless networks. Jamming is the problem can be occurred in end to end communication/transmission in

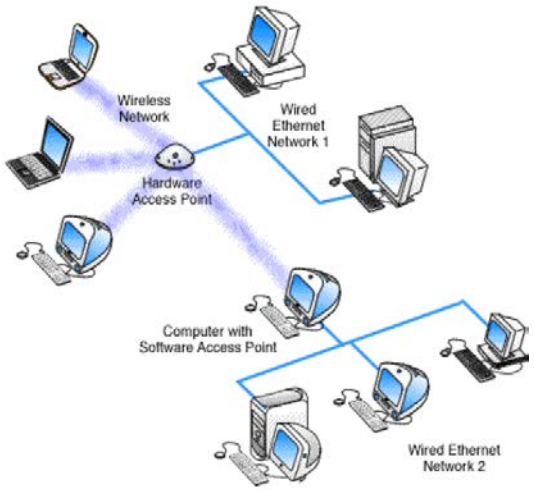

Fig. 1: Wireless sensor network architecture

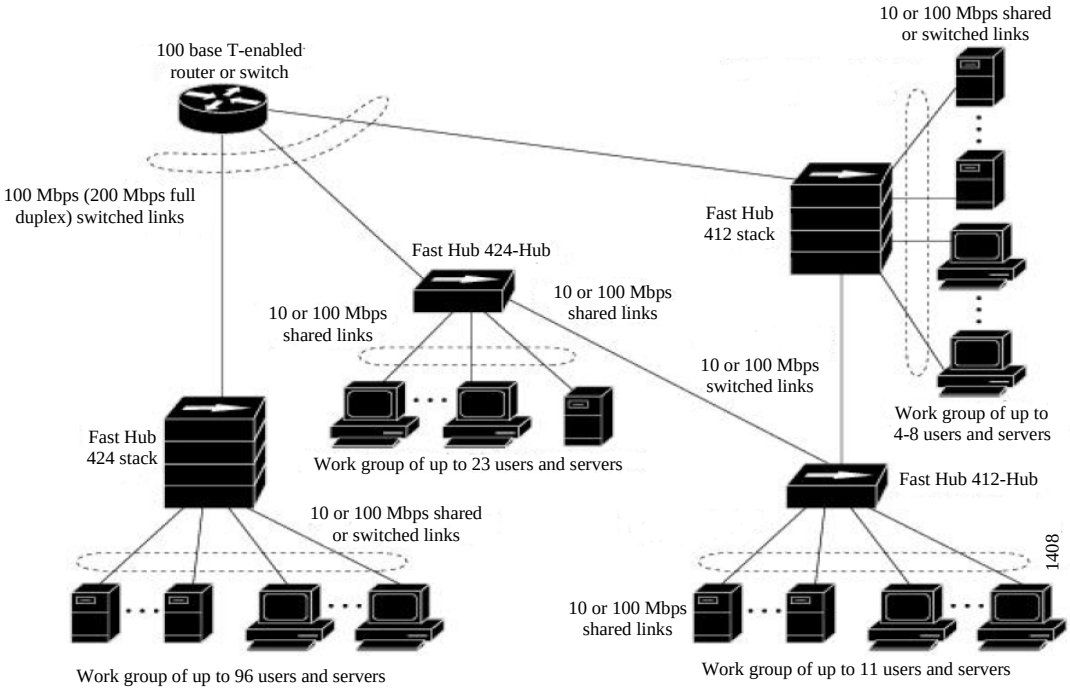

Fig. 2: Jamming architecture through routers

wireless sensor network (Souza *et al*., 2013). The changes of the jamming at the physical layer resonate through the protocol hierarchy present in wireless sensor network through wireless networks.

As shown in Fig. 2 the simplest methods were defined for providing anti jamming properties to the wireless sensor networks. Anti jamming methods measures have been into higher layers for data transmission to various channels in wireless networks. The sample anti jamming protocols may introduce different MAC channels, multiple routing paths for detecting adversary protections form jamming attacks. Traditionally developed security techniques are not suitable data transfer in network with increasing network performance through protocol properties. Packet hiding methods were developed traditionally for application construction with suitable data transfer between every user present in wireless networks. But compromised nodes are providing way to abnormal user's identity. So, in this Intrusion and detection were used for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of the adversary risking exposure. Due to this to make use of routing diversity in this achievement each source node must be able to make an intelligent location of traffic across the available paths through the network jamming detection.

Literature review: This chapter is based on previous research that we have discussed the changes of outside selective jammer targets various control packets in various data links present in the sub layer of data link layer (Proano and Lazos, 2012). By using above sequence to perform classification include to adversary exploits insert in to packet timing information for packet data transfer procedures with transmissions. Based on the network traffic analysis the inter packet transmission times for various packet types. This is called as probability distribution by Kolluru *et al*. (2016), Law etc. Later the prediction of estimation timing information is done on various data transmissions. Based on the above requirements the authors proposed selective jamming techniques for traditional MAC layer protocols.

Several researchers have been introducing channel selective jamming attacks, in which the jammer targets the broadcast controlling channels. It has shown that shown attacks reduce required power for performing a DoS attack by several orders of magnitude. To control channel accessing that reduces traffic allocated in controlling of transmission.

MATERIALS AND METHODS

Problem statement: In wireless networks the data packets are following these types:

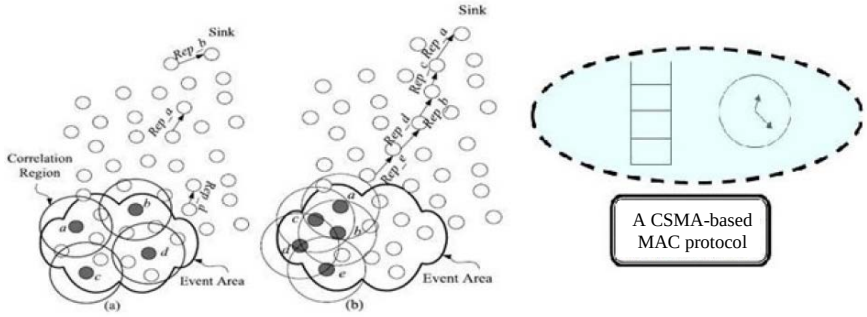

Fig. 3: MAC layer protocol efficiency

- Route Request (RREQ)
- Route Reply (RREP)
- Route Error (RERR)
- Route Reply Acknowledgment (RREPACK)

Firstly jamming will detect and identify the activity of jamming which defines the transferring the data within the network. It is not a transmitonly activity. In the wireless sensor networks the every layer and every node needs to sensor the packet information. But in wireless sensor networks it is not recommended to show the packet information to all the nodes. To hide the packet information in wireless sensor networks many packet hiding algorithms are implemented in this study. By using this approach information of the every packet is encrypted within the network. By using 802.11 the network can identified weather a packet has jammed or not and node send the data loss packet within 9 msec (Royer and Perkins, 1999). Generally, jamming is not identified within the network by using threat exception protocol. At this situation jamming plans to identify the networks continuously and randomly for the transmission of high-power interference signal transmission between nodes present in wireless sensor networks.

In this model, adversary hub can accomplish to grow a lot of methodology to stick recurrence groups of intrigue and afterward constant to nearness of abnormal high obstruction levels makes the sort of assaults simple to recognize. Customary hostile to sticking methods depend widely on spread-range (SS) correspondences or some type of sticking avoidance (e.g., slow frequency hopping or spatial retreats). Above strategies show bit level insurance by spreading bits into mystery pseudo clamor code to the correspondence parties. These strategies are relevant for just secure remote transmissions under the outside string model Fails to efficiently handle internal threat models (Ratna and Ravi, 2015). So, a better jamming detection system is required to handle internal threat models. An efficient comparative schema was developed based on symmetric cryptographic techniques such as AES/DES is used to prevent selective jamming in the wireless sensor networks. A model that utilizes enemy filtration at the season of system joining however traded off routers is a superior method for averting jamming before it can really happen. So, a better system is required that implements this claim.

Our approach: Still uses Wireless networks driven by reactive protocols containing RREQ, RREP, RERR, RREP-ACK message packets (Sohrabi *et al*., 2000). Proposes to use commitment schemes along with intrusion detection techniques for identifying compromised routers Algorithm 1.

Algorithm 1; Packets information:

Input: Packets information
Output: Data encrypted with buffer size information.
Step 1: The data is divided into 64 bits.
Step 2: The length of the original message into 64 bit)
Step 3: Construct Pre-Processing methods like
f(t; X, Y,Z) = (X AND Y) OR ((NOT X) AND Z) (0 <= t <= 19)
f(t;X, Y, Z) = X XOR Y XOR Z (20 <= t <= 39)
f(t;X,Y,Z) = (X AND Y) OR (X AND Y) OR (X AND Y) (40 <= t <=59)
f(t;X,Y,Z) = X XOR Y XOR Z (60 <= t <= 79)
Step 4: The original message is related to constant
K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)
Step 5: Depending on the number of words the buffer sizes are taken
A0 = 0x76554521
A1 = 0xPQRXY91
A2 = 0x97QPRXYZ
A3 = 0x2123121
A4 = 0xY3Z2Q1P0
Step 6: Processing of message in 512 bit blocks
K(0), K(1), ..., K(79): 80 Process Static Words
A0, A1, A2, A3, A4, A5: 5 Initial values with buffering words

Secure hash function algorithm for cipher text generation is shown in Fig. 3 input message can be

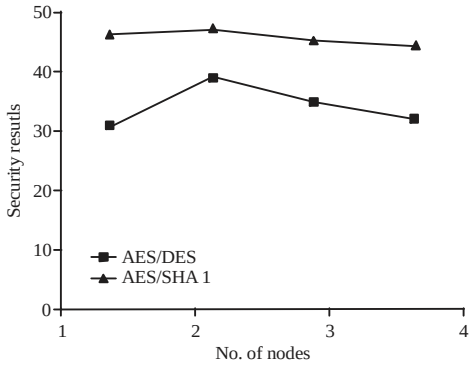

Fig. 3: Comparison results with existing and proposed approaches

converted into cipher text generation using cryptographic features in network communications (Berger *et al*., 2016). By using above sequence we will provide more security considerations based on the process states.

To solve the efficient cryptographic problems are achieved for decreasing the time consuming assurance present in network communications (Dong *et al*., 2013). Further capable of accessing physical derived network devices and recovery stored information including cryptographic keys and PN codes for data transfer between nodes present in network (Fig. 4).

RESULTS AND DISCUSSION

Performance analysis: This study describes the efficiency of the network performance into considerable data transmission in wireless networks. Construct network with number of nodes using the ip address and port number of the service provider present base station process for transferring data from sender to receiver process. In this study, we construct Jamming node for data construction with equivalent data transfer between each node present in the wireless networks.

As shown in Fig. 4 traditionally used encryption and decryption process for providing security solutions but other nodes are comprised to every node present in the wireless sensor networks. In this study, we propose to extend our proposed to existing approaches like AES and DES algorithms, to provide efficient security in real time data transfer from service provide to other nodes present in the network.

CONCLUSION

The wireless network is used to transfer the data from source to destination by using nodes. Several attack models have been addressed in this research to detect the attackers and solve the jamming issues with in the wireless networks. In our research, several packet classifications algorithms have been discussed. In this study, the data transfer is based on RREQ and RREP packets from the preview of the adversary selective jamming. The proposed system detect the compromised routers to improve the efficiency of the overall network. Our experimental show efficient implementation validates to users claim data. As further improvement of our proposed work is to provide efficient data transfer in network using advanced algorithms present in the network processing.

REFERENCES

Benyamina, D., A. Hafid and M. Gendreau, 2012. Wireless mesh networks design a survey. IEEE. Commun. Surv. Tutorials, 14: 299-310.

Berger, D.S., F. Gringoli, N. Facchi, I. Martinovic and J.B. Schmitt, 2016. Friendly jamming on access points: Analysis and real-world measurements. IEEE. Trans. Wireless Commun., 15: 6189-6202.

Dong, Q., D. Liu and M. Wright, 2013. Mitigating jamming attacks in wireless broadcast systems. Wirel. Networks, 19: 1867-1880.

Kolluru, P.K., P.S. Vijaya, M. Anusha, B.S. Razeena and M. Sowjanya, 2016. An efficient cognitive radio network technique to share spectrum by using optimal power allocation. Asian J. Inf. Technol., 15: 4602-4607.

Proano, A. and L. Lazos, 2012. Packet-hiding methods for preventing selective jamming attacks. IEEE. Trans. Depend. Secure Comput., 9: 101-114.

Ratna, S.R. and R. Ravi, 2015. Survey on jamming wireless networks: Attacks and prevention strategies. World Acad. Sci. Eng. Technol. Intl. J. Comput. Electr. Autom. Control Inf. Eng., 9: 642-648.

Royer, E.M. and C.E. Perkins, 1999. Ad hoc on-demand distance vector routing. Proceedings of the IEEE 2nd International Workshop on Mobile Computer Systems and Applications, February 25-26, 1999, IEEE Computer Society Washington, DC, USA., pp: 90-100.

Sohrabi, K., J. Gao, V. Ailawadhi and G.J. Potie, 2000. Protocols for self-organization of a wireless sensor network. IEEE Pers. Commun., 7: 16-27.

Souza, E., H.C. Wong, I. Cunha, A.A. Loureiro and L.F.M. Vieira *et al*., 2013. End-to-end authentication in under-water sensor networks. Proceedings of the 2013 IEEE International Symposium on Computers and Communications (ISCC), July 7-10 2013, IEEE, Split, Croatia, pp: 000299-000304.