International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 7
ISSN: 2454-4248
03 – 08

Defeating Jamming Attack in Wireless Ad-Hoc Networks using Puzzle Based Hashing Technique

T.Aruna[1]
Research Scholar
Dept.of Computer Applications
Alagappa University,
Karaikudi.
raamirtha@gmail.com[1]

R.Anandha Jothi[2]
Research Scholar
Dept.of Computer Applications
Alagappa University,
Karaikudi.
ranandhajothi12@gmail.com[2]

V.Palanisamy[3]
Professor & Head
Dept.of Computer Applications
Alagappa University,
Karaikudi.
vpazhanisamy@yahoo.co.in[3]

Abstract— The growth of wireless technologies, jamming in wireless sensor network is a major problem in network communication. Jamming attacks is a denial of service (DoS) attack in network to block legitimate communication. Wireless networks drop multiple security threats. Transceiver can intrude on wireless transmissions under cryptographic methods. In jamming, the message is transmitted as continuous transmission of high signals. These strategies have many disadvantages. We have to increase the energy of jam frequency and easy to detect attacks. Normal anti-jamming techniques depend on spread-spectrum communications. This technique is used to secure only wireless transmission. To deeply understand this above problem, we need to analyze in detailed manner. Finally we discuss open issues in this network, such as energy efficient saving scheme, packet classification and packet dropping.

Keywords- *AODV, Wireless Networks, Packet Classification, Packet dropping, Jamming Attack.*

*****

I. INTRODUCTION

Wireless sensor network have a huge amount of low power sensor nodes. These low power sensor nodes are used for low energy saving and low cost. The real time application for these network is military, environment monitoring, etc. These application wants to secure their data. Wireless networking is a main role to achieve universal computing where network devices are binded in environment provide unbroken connectivity and services. However due to the exhibit nature of wireless links. Wireless networks are easily attacked by jamming concept. Jamming can create Dos problem, which may cause several security problem.

Jamming is one of the DoS attacks. In this attack, jamming devices and electromagnetic energy are needed to prevent signal transmission. Different types of jammer are categories as follows, In constant jammer, it gives uninterrupted signals in wirelss network. MAC protocol is inefficient for this jammer. In deceptive jammer, the transmitted bits are not random bits, it is effective one[1]. In random jammer, it is more energy than constant and deceptive jammer. In reactive jammer, it is very effective compared with constant and deceptive jammer. Jamming is the main problem in main applications. For example, in border security, a hacker has the ability to secure the communication without detected. In unwanted environment, to detect the place where the channel is jammed.

Wireless networks drop multiple security threats. Transceiver can intrude on wireless transmissions under cryptographic methods [12, 13]. Jamming attacks are complicated to count the attacks. They have to visualize Dos attack opposed on wireless network. In jamming, the message is transmitted as continuous transmission of high signals. These strategies have several disadvantages. We have to increase the energy of jam frequency and easy to detect attacks [14]. Normal anti-jamming techniques depend on spread-spectrum communications. This technique is used to secure only wireless transmission. To identify how a jammer attacks in wireless network and how to restrict jamming to achieve well-organized communication, we investigate three different characteristic of wireless network jamming, one is, previous jamming types and another one is protocol for jammers and finally jamming detection. First a network can be jammed in several ways in different jamming types. To remove jamming in network, we should know how jammer works. For that reason, we discuss different types of jammers.

In previous studies, it takes longer time to find packet dropping. The research work is mainly focus to detect jamming attack in wireless sensor network using symmetric cryptography, packet classification.

II. ROUTING PROTOCOL AND TYPES OF ATTACKS

A. AODV Routing Protocol.

The AODV reactive protocol as it is an efficient low-overhead approach. This relies on the underlying assumption that all nodes are trustworthy and will never deviate from the protocol. In this work we do not make this assumption, and use trust to militate against malicious or faulty behavior. Accordingly, association based routing which is to be applied over the AODV protocol in order to enhance the protection. The objective of this TB-DRI is to fortify the existing

 ISSN: 2454-4248
03 – 08

implementation by selecting the best and secured route in the network. Further this routing is strengthened by verification mechanisms.

MANET is a configured network consists of mobile nodes that communicate through a wireless medium in the lack of any centralized control of the network[2]. Each node can move without restraint in space. Therefore, the topology of the network changes dynamically a MANET can be constructed quickly at a little cost. MANET has a vibrant topology such that nodes can easily join or leave the network at any instance[3,4]. They have more possible applications, mainly, in military and rescue areas such as linking soldiers on the battlefield or creating a new network in place of a network which collapsed after a disaster like an earthquake and flood.

B. Jamming Attack

Wireless networks drop multiple security threats. In wireless transmissions message can secured under cryptographic methods. They have to display Dos attacks. In simple jamming, messages are transmitted a continuous jamming signal. In external jamming model, jamming scheme holds continuous or random transmission signals. There are several disadvantages are adopting this model[6]. We have to improve the energy of jam frequency. Second one is easy to find attack. Traditional anti-jamming techniques are depending on spread spectrum communications. This technique protects only bit-level on wireless transmission.

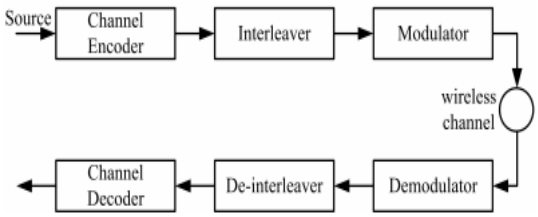

Fig.1. Communication System

In this paper predict jamming in internal thread model. In selective jamming attacks, we give the importance to specific messages[5]. If the jammer can aimed to reduce the throughput of route request and reply message in TCP. Selective jamming attacks, the receiver follow classify and jam model before the end of wireless transmission[7,8]. These strategy, classify delivery packets and decode it. In the first packets holds the type of packet, size of packet and address of source and target. So, selective jamming is necessary to strong knowledge on physical layer and as well as above layers. In this work includes jamming attacks, puzzle based jamming scheme and classification, verification and finally conclusion.

III. RELATED WORK

S.M. Bamakan, H. Wang, T. Yingjie, Y. shi, An effective interruption identification framework is depend on mclp/svm. Several companies accept the usage of knowledgeable tools and systems to secure their system network and minimize the danger of yielding their information details. Even though several machine learning classification algorithms are introduced in network interruption identification problem, every technique has plus-point and negative point. In this paper we propose an interruption identification problem framework using flexible, strong simplifying method called time-varying optimization. Support Vector Machine (SVM) provides high detection rate compared with other features.

Yaqoob, E. Ahmed, M. H. Rehman, A. I. A. Ahmed, M. A. AlGaradi, M. Imran,M. Guizani, Previous security mechanisms are little more applicable because of resource-constrained devices. These devices need more computation power and resources. This paper initiates the ransom ware attacks and security concerns. We initially discuss the growth of ransom ware attacks. We explore report and highlight the research effects from security outlooks. A concept is devised by dividing and categorizing the literature based on important input parameters. Additionally, a few acceptable case studies are outlined to intimate the people.

IV. CRYPTOGRAPHIC PUZZLE HINDING SCHEME FOR JAMMING ATTACK

We give the importance of selective jamming attack. We use opnet tm modeler 14.5 model to acheive selective jamming attack in multi-hop wireless network. Jammers are not easy to detect by the user. Wireless links and wireless networks are simply attacked under jamming technology[9]. For that reason, we use puzzle-based on hashing techniques. In first phase, the attackers find TCP connection in multi-hop wireless network. In second phase, jammer find network layer control messages in route selection process.

In selective jamming, we prepare to send the 3mb file content to two users in muli-hop under the usage of TCP protocol. The contend transmission rate is 11 mbps. We use 4 jamming strategies that are, cumulative tcp and acks, rts and cts message and data packets and finally random jamming. Throughput leaves on random and selective jamming[10]. tcp and acks are translated under congestion control. The sender translate the loss packets without leave the size of packet. Our new approach to find malicious node in data transmission without leave the packet[11].

A. Cryptographic Puzzle Hiding Scheme (CPHS)

In this scheme, we assume sender s1 hold packet p for data transmission. Sender choose a random key m1∈ {0, 1}s1, for a packet length. s1 creates a puzzle p1=puzzle(k1,t_p), here puzzle() indicate puzzle creation function and t_p indicates time for puzzle. t_p is depend on computational capability of receiver indicated by N. Sender send(c1,p1), where c1=Ek (π1(m1)) and receiver R1 received puzzle p1 by recover key then computes m1= π-1(D_k'(c1)). If the decoded packet m1 is proper format, otherwise remove m1 packet.

B. Packet Classification

The starting node starts to find process by transmitting packet to opposite node. The malicious node is a one sector of network and received RREQ. The starting node starts forwarding; we define how the received can split packets before sending the packet on transmission. If the packet is splitted, the receiver may pick to jam rely on above strategy. Let's assume generic system in the physical layer, packet p1 is encoded format and interleaved it and finally modulated

 ISSN: 2454-4248
03 – 08

format before transmitted packet in channel. At the receiver side, the signal is demodulated format and interleaved it and finally decoded to gather original packet p1. The receive ability to split the data in packet p1 reply on creation of block. If the channel encoding part extends original data bit sequence m1, repetitions for securing channel error. A α/β-block may secure m1 from error e1 from each packet.

V. IMPLEMENTATION OF PUZZLE BASED ON HASHING TECHNIQUE

We consider many puzzle schemes to define security and performance. Crytographic puzzle technique is used to protect in insecure channel. To secure Dos attacks using broad cast and key escrow techniques. Time lock puzzles are used to control the many modulo operation.

Time lock puzzles techniques have many advantages to control tp. The puzzle generation function need low computation estimated with puzzle solving. In time lock puzzle, the puzzle generation function generates g1= u1 • v1, where u1 and v1 are prime numbers. They choose a random r, 1 < r < g1 and kept out the encryption key in Kh = k 1+ r2 t1 mod g1, where t1 = tp • M is used to solve the difficult of k1. Here, kh generates φ(g1) = (u1 − 1)(v1 − 1). Puzzle includes P1 = (g1, Kh, t1, r). In this work, modulo g1 is called as prioi. If the sender may drop the puzzle information in (Kh , t1, r). Here puzzles rely on hashing concept. If the receiver may suffer notable delay and energy saving where using modulo function. For that reason, this scheme is implemented using cryptographic puzzles.

VI. RESULTS AND DISCUSSION

The simulation is implemented In Network Simulator-2, a simulator for wireless networks. In the existing system, their use packet hiding methods and selective jamming, classification of jammers, packet dropping concept but their achieve 96% result of packet hiding. But, in the proposed system, we implement Puzzle based on hashing technique and Symmetric cryptography so we achieve 98% result of packet hiding.

In this paper predict jamming in internal thread model. In selective jamming attacks, we give the importance to specific messages[5]. If the jammer can aimed to reduce the throughput of route request and reply message in TCP. Selective jamming attacks, the receiver follow classify and jam model before the end of wireless transmission[7,8]. These strategy, classify delivery packets and decode it. In the first packets holds the type of packet, size of packet and address of source and target. So, selective jamming is necessary to strong knowledge on physical layer and as well as above layers. In this work includes jamming attacks, puzzle based jamming scheme and classification, verification and finally conclusion.

VII. CRYPTOGRAPHIC PUZZLE HINDING SCHEME FOR JAMMING ATTACK

We give the importance of selective jamming attack. We use opnet tm modeler 14.5 model to acheive selective jamming attack in multi-hop wireless network. Jammers are not easy to detect by the user. Wireless links and wireless networks are simply attacked under jamming technology[9]. For that reason, we use puzzle-based on hashing techniques. In first phase, the attackers find TCP connection in multi-hop wireless network. In second phase, jammer find network layer control messages in route selection process.

In selective jamming, we prepare to send the 3mb file content to two users in muli-hop under the usage of TCP protocol. The contend transmission rate is 11 mbps. We use 4 jamming strategies that are, cumulative tcp and acks, rts and cts message and data packets and finally random jamming. Throughput leaves on random and selective jamming[10]. tcp and acks are translated under congestion control. The sender translate the loss packets without leave the size of packet. Our new approach to find malicious node in data transmission without leave the packet[11].

A. *Cryptographic Puzzle Hiding Scheme (CPHS)*

In this scheme, we assume sender s1 hold packet p for data transmission. Sender choose a random key m1∈ {0, 1}s1, for a packet length. s1 creates a puzzle p1=puzzle(k1,t_p), here puzzle() indicate puzzle creation function and t_p indicates time for puzzle. t_p is depend on computational capability of receiver indicated by N. Sender send(c1,p1), where c1=Ek (π1(m1)) and receiver R1 received puzzle p1 by recover key then computes m1= π-1(D_k'(c1)). If the decoded packet m1 is proper format, otherwise remove m1 packet.

B. *Packet Classification*

The starting node starts to find process by transmitting packet to opposite node. The malicious node is a one sector of network and received RREQ. The starting node starts forwarding; we define how the received can split packets before sending the packet on transmission. If the packet is splitted, the receiver may pick to jam rely on above strategy. Let's assume generic system in the physical layer, packet p1 is encoded format and interleaved it and finally modulated format before transmitted packet in channel. At the receiver side, the signal is demodulated format and interleaved it and finally decoded to gather original packet p1. The receive ability to split the data in packet p1 reply on creation of block. If the channel encoding part extends original data bit sequence m1, repetitions for securing channel error. A α/β-block may secure m1 from error e1 from each packet.

VIII. IMPLEMENTATION OF PUZZLE BASED ON HASHING TECHNIQUE

We consider many puzzle schemes to define security and performance. Crytographic puzzle technique is used to protect in insecure channel. To secure Dos attacks using broad cast and key escrow techniques. Time lock puzzles are used to control the many modulo operation.

Time lock puzzles techniques have many advantages to control tp. The puzzle generation function need low computation estimated with puzzle solving. In time lock puzzle, the puzzle generation function generates g1= u1 • v1, where u1 and v1 are prime numbers. They choose a random r,

 ISSN: 2454-4248
03 – 08

1 < r < g1 and kept out the encryption key in Kh = k 1+ r2 t1 mod g1, where t1 = tp • M is used to solve the difficult of k1. Here, kh generates φ(g1) = (u1 − 1)(v1 − 1). Puzzle includes P1 = (g1, Kh, t1, r). In this work, modulo g1 is called as prioi. If the sender may drop the puzzle information in (Kh , t1, r). Here puzzles rely on hashing concept. If the receiver may suffer notable delay and energy saving where using modulo function. For that reason, this scheme is implemented using cryptographic puzzles.

IX. Results and Discussion

The simulation is implemented In Network Simulator-2, a simulator for wireless networks. In the existing system, their use packet hiding methods and selective jamming, classification of jammers, packet dropping concept but their achieve 96% result of packet hiding. But, in the proposed system, we implement Puzzle based on hashing technique and Symmetric cryptography so we achieve 98% result of packet hiding.

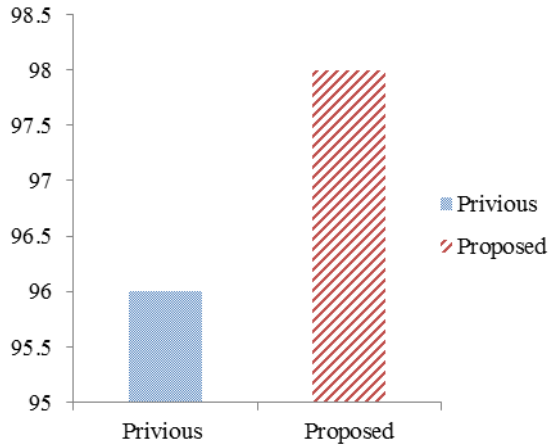

Fig.1. Performance comparison of Previous and proposed work

X. VERIFICATION

Implementation of wireless node in NS-2 with AODV, Implementation of jamming attack with selective transmission, Implementation of packet classification for wireless traffic, Implementation of packet hiding for real packet using wireless network 50 nodes, Detection of jamming attack and analysis with throughput. The model is shown in Fig. 2.

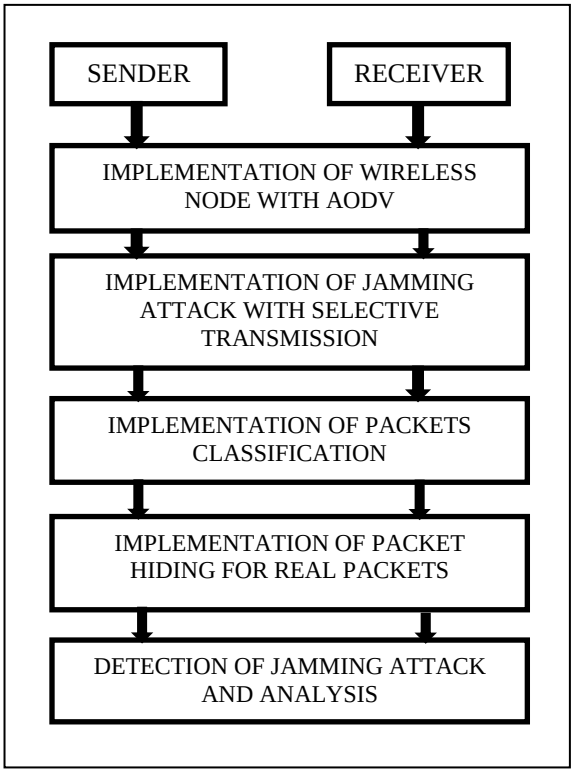

Fig. 2: Block Diagram of the proposed system.

Algorithm for packet sending

```
Received request packet
if(this request already processed)then
/*nothing to do with this request*/
return;
else
/*check timer whether it is running*/
if(delay not zero)then
set timeout to delay;
start timer;
else
select random_back-off_time
set timeout to random_back-off_time
start timer
/* listen to on going traffic */
while (timeout not equal zero)
{
if(hear re-broadcast of this
request from other nodes)then
set delay to remaining time
return;
end if
}
switch to forwarding node
set request packet processed to TRUE
return;
end if
end if.
```

XI. SIMULATION SETUP

The simulation is implemented In Network Simulator-2, a simulator for wireless networks. The simulation parameters are given in the following table

Parameter	Value
Studied Protocol	AODV
Transmission range	250m
Packet size	1024 bytes
Area	1000 X 500
Transmission Interval	0.1 ms
Simulation Duration	10 ms
Number of nodes	30
Antenna Type	Omni Antenna
Initial Energy	100 ules

XII. CONCLUSIONS

In this paper, puzzle based hashing techniques were applied to defeating Jamming attack has been studied effectively. A security protocol has been proposed to identify the ways of packet dropping nodes in MANET and thereby redirecting a safe routing path from source node to the destination node avoiding the malicious nodes. The results have been simulated with ns-2 and compared with the AODV and puzzle based on hashing security mechanism. We planned to work in future on packet dropping attack with different routing protocols for security in MANET and simulated using ns-2.

ACKNOWLEDGMENT

This article has been written with the financial support of RUSA-Phase 2.0 grand sanctioned vide Letter No.F.24-51/2014-U. Policy (TNMulti-Gen).Dept. of Edn. Govt.ofindia, Dt.o9.10.2018.

REFERENCES

[1] R. Ananadha Jothi, V. Palanisamy, " Trust Based Association Estimation Technique on AODV Protocol Against Packet Droppers in MANET", International Journal of Applied Engineering Research,10 (55) (2015) 2408-2413.

[2] R. Ananadha Jothi, V. Palanisamy, "Various Attacks and Its Countermeasures in Mobile Ad Hoc Networks" , A Survey International Journal of Engineering Research & Technology,3 (3) (2014) 50-57.

[3] [3] J. Nithyapriya, R. Ananadha Jothi, V. Palanisamy, " Securing data with selective encryption based DAC scheme for MANET", Computer Networks, Big Data and IoT, (Springer) Dec- 2018 (Accepted).

[4] J. NithyaPriya, R. Anandha Jothi, V. Palanisamy, "Security scheme for MANET based on echoing and path changing", International Journal of Innovative science and research technology, 3 (10) (2018) 601-603.

[5] M. Jeevamaheswari, R. Anandha Jothi, V. Palanisamy, "AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET", International Journal of Scientific Research in Science and Technology, 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X.

[6] G. Morabito, " Exploiting the Timing Channel to Increase Energy Efficiency in Wireless Network", IEEE J.Sel.Area Commun| Volume 29| no.8 | pp.1711-1720, sep.2011.

[7] L. Galluccio, G. Morabito, S. Palazzo, "TC-A Novel Access Scheme for Wireles Networks With Transmit-only Nodes", IEEE Trans.Wireless Commun | Volume 12 | no.8 | pp.3696-3709, aug. 2013.

[8] W. Xu, W. Trappe, Y. Zhang, " Anti-Jamming Timing Channels for Wireless Network", inproc.1st ACM Conf. Wireles Netw.Security, 2008, pp.203-213.

[9] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, " Efficiency Analysis of Jamming-based Countermeasures Against Malicious Timing Channel in Tactical Communication", inproc.IEEE ICC, 2013, pp.4020-4024.

[10] W.Xu, K. Ma, W. Trappe, Y. Zhang,, "Jamming Sensor Networks: Attack and Defense Strategies", IEEE Netw | Volume 20 | no.3 | pp. 41-47, may/jun 2006.

[11] R.Saranyadevi, M. Shobhana, D. Prabakar, " A Survey on Preventing Jamming Attacks in Wireless Communication", Int.comput.Appl., Vol. 57, no.23, pp. 1-3, nov.2012.

[12] V.Palanisamy. Laveen Sundararaj "Delay Tolerant Networking Routing as a Game Theory problem – An Overview" International Journal of Computer Networks July 2(3)2010, pp:160-172.

[13] V Palanisamy, P Annadurai, S Vijayalakshmi "Impact of black hole attack on multicast in ad hoc network (IBAMA)", IEEE International Conference on Computational Intelligence and Computing Research.2010 pp:1-4.

[14] M Lalli, V Palanisamy, "A novel intrusion detection model for mobile ad-hoc networks using CP-KNN" International Journal of Computer Networks & Communications (IJCNC) vol- 6(5) ,2014, pp193-201.

Ms. T.Aruna is a currently pursuing M.Phil degree in Network Security at Department of Computer Applications in University, Karaikudi, Tamil Nadu, India. She was completed B.sc(INFO TECH) and also complited M.C.A., degree. She do projects in biometrics, networks and security. Her main research involved in thrust areas such as Network Security and Ad-Hoc Networking. She has attended some international Conferences Corresponding. Her main areas of research includes Network based security. She has published her research article in UGC approved journal. Author: E-Mail: aruna1995mca@gmail.com.

Mrs. R. Anandha Jothi is a Project Fellow under the scheme of Rashtriya Uchchatar Shiksha Abhiyan (RUSA)-PHASE 2.0, Govt. of India and pursuing Ph.D degree in Biometrics at Department of Computer Applications at Alagappa University, Karaikudi, Tamil Nadu, India. She was completed M.C.A., and M.Phil.

 ISSN: 2454-4248
03 – 08

degree in Alagappa University, Karaikudi, Tamil Nadu, India. Her main research involved in the thrust areas such as Network Security, Image Processing, Pattern Recognition and Ad-Hoc Networking. She has published more than 30 research articles in reputed scopus indexed International Journals and attended more than 15 International Conferences.

E-Mail: ranandhajothi12@gmail.com.

Dr.PalanisamyVellaiyan obtained his B.Sc degree in Mathematics from Bharathidasan University in 1987. He also received M.C.A. and Ph.D. Degree from Alagappa University in 1990 and 2005 respectively. After working as Lecturer in AVVM Sri Pushpam College, Poondi Thanjavur from 1990 to 1995, He joined Alagappa University as Lecturer in 1995. He is currently working as Professor and Head of the Department of Computer Applications and Dean Student Affairsof the Alagappa University. He also received M.Tech. Degree from Bharathidasan University in 2009. He has published more than 170 international journals and he has attended 25 national conferences and 60 international conferences and his research interest includes Computer Networks & Security, Data Mining & Warehousing, Mobile Communications, Computer Algorithms and biometrics.

E-Mail : vpazhanisamy@yahoo.co.in.