Middle-East Journal of Scientific Research 24 (6): 2013-2021, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.06.23586

A Novel Approach for the Detection of Jamming Attacks in MANET Using Game Theory Based Defense Technique

[1]S. Vadhana Kumari and [2]B. Paramasivan

[1]AP/CSE, Maria College of Engineering & Technology, Attoor,
Thiruvattar P.O., Kanya Kumari. Dist, Tamil Nadu, India
[2]National Engineering College, Kovilpatti, Thoothukudi Dist. Tamil Nadu, India

Abstract: In MANET a group of mobile hosts with wireless network boundaries form an impermanent network without the assistance of any fixed infrastructure or integrated management. In this paper we proposed a co-operative combined Defense Technique for detection of Jamming Attacks. Here for detection of jamming attacks we have used Correlation Coefficient (CC) of two communicating nodes. Thus the Correlation coefficient is between the reception error time and the correct reception time and if the Correlation coefficient (CC) is larger than produced relative Error Probability (EP) then the network is recognized as jammed. Thus the proposed scheme can detect only Reactive Jammer by correlation coefficient among the reception error time and the correct reception time and to elaborate the efficiency of the technique beside with CC, we use Carrier Sensing Time, Packet Delivery Ratio (PDR) and signal strength (SS).

Key words: Jamming Attack · Correlation coefficient · Packet Delivery Ratio · Signal Strength

INTRODUCTION

Manet: A Mobile Ad Hoc Network (MANET) is combination of wireless mobile nodes. These nodes may move unpredictably to forming a temporary network without any fixed backbone infrastructure. In MANET the network topology may change rapidly and unpredictably over time because the nodes are mobile. This is a decentralized network [1]. In MANET mobile servers and clients can communicate with each other directly through wireless link in the absence of fixed wired infrastructure [2]. There are various applications of MANET like video conferencing, rescue operations, military applications, Disaster Management etc

Jamming Attack: Jamming is an act of purposely directing electromagnetic energy towards a communication system to interrupt or prevent signal transmission. Jamming is attack interferes with the radio frequencies used by network nodes [3]. In Jamming attack adversaries try to overpower transmitted signals for this they inject a high level of noise, thereby lowering the signal-to-noise ratio (SNR). Lowering the SNR, in turn, can considerably decrease the achievable rate of a communication system [4]. In jamming, the opponent interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Normally, jamming attacks are considered under an external threat model, in which the jammer is not part of the network [5].

Types of Jammer: There are several types of jamming attacks which are discussed below.

Constant Jammer: The constant jammer are that types of jammer which emits a radio signal continually and can be implemented using either a waveform generator which continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer protocol. A constant jammer can well prevent genuine traffic sources from getting hold of a channel and sending packets.

Deceptive Jammer: The deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions and does not

Corresponding Atuthor: S. Vadhana Kumari, AP/CSE, Maria College of Engineering & Technology, Attoor, Thiruvattar P.O., Kanya Kumari. Dist, Tamil Nadu, India.

send out random bits. As a result, a normal communicator will be take into believing there is a legal packet and be swindle to remain in the receive state.

Random Jammer: A random jammer alternates between sleeping and jamming in place of continuously sending out a radio signal. Generally it jammed the system for a while after that it turns off its radio and enters a "sleeping" mode. After sleeping for some time, it resumes jamming. It can behave like either a constant jammer or a deceptive jammer during its jamming phase. This jammer model tries to capture energy conservation into consideration, which is chiefly important for that type of jammers that do not have unrestricted power supply.

Reactive Jammer: The reactive jammer are that types of jammers which stays calm when the channel is idle and starts transmitting a radio signal as soon as it senses activity on the channel. The reactive jammers are harder to detect [6].

Jamming Attack Detection: There are a number of Jamming Attack Detection statistics that logically provide themselves to detecting jamming, which are the following.

Signal Strength Measurement: Signal strength measurement can be employed to detect jamming. The signal strength distribution may be affected by the presence of a jammer so Signal strength measurement can detect jamming attacks. Two natural approaches to detecting jamming using signal strength occupy comparing average signal magnitude vs. a threshold calculated from the ambient noise levels and categorize the shape of a window of signal samples.

Carrier Sensing Time: Jammer can prevent a genuine source from sending out packets because jammer shows a genuine source that the channel is constantly busy to the source and hence it might seem possible to use carrier sensing time as a means to find out whether a device is jammed. Use of carrier sensing time is appropriate under the following two conditions that are: the jammer is non-reactive or non-random and the primary MAC protocol decides whether a channel is idle by comparing the noise level with a fixed threshold.. If these two conditions are true, then the carrier sensing time is an efficient way to discriminate a jammed scenario from a normal ill-functioning scenario.

Packet Delivery Ratio: The jammer can effectively corrupt transmissions, leading to a much lower Packet Delivery Ratio so the Packet Delivery Ratio may be used to detect the presence of jamming. Since a jamming attack will corrupt the channel quality surrounding a node, the detection of a radio interference attack basically boils down to determining whether the communication node can send or receive packets in the way it should have the jammer not been present [6].

Need for Jamming Attack Detection: Detection of jamming attacks is very important because it is the basic requirement to building a secure and dependable wireless network [7]. WLANs are constructing by shared medium which makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. Jumping of channels is one of the most efficient ways to detect jamming attack. Because communication between two genuine nodes is done throughout a definite frequency, the frequency can be changed if necessary. While a jammer is attacking the wireless network, there are other effective ways to continue genuine communication in the network [8]. The IEEE 802.11b standard has a Clear Channel Assessment (CCA) in DSSS protocol. This protocol checks whether WLAN channel is free for transmitting. Using the same protocol in IEEE 802.14.5 will only put at risk the performance of the network. So for secure the link from intruders detection of any attack is important [9]. Jamming attacks should be detected to fulfill all responsibilities and maintain all functions for a Network [10]. The development of detection and reaction mechanisms of jamming nodes is necessary for providing Secure interrupted communication. Detecting a jamming attack is not easy in IEEE 802.11n because it is not possible to differentiate a collision with a bad SNR [11].

Avoidance of Jamming Attack: Intrusion Prevention Systems try to prevent jamming by either avoiding or fighting against the malicious entities.

Frequency Hopping: Frequency hopping has been traditionally employed for overcome the presence of a jammer. Frequency hopping can be either reactive or proactive. In the reactive Frequency hopping, when a node finds that it is jammed then it switches to a different channel and sends a beacon message on the new channel to announcing its presence. Its non-jammed neighbors

sense its absence and change their bands of operation to check if their lost neighbor has sent beacons announcing its presence on a different channel. If they don't find beacons announcing presence of node on a different channel, then they assume that the node just moved away. If they sense a beacon, they inform the other nodes in the network to change channels. In proactive frequency hopping protocol there is pseudo-random channel switching.

Spatial Retreats: In Spatial Retreats Mobile nodes affected by the jammer can move away from their initial positions to avoid jamming signals. In this method when a node notices that it is being jammed, then this node tries to get away from the jammed area (evasion phase) and stay connected with the rest of the network (reconstruction phase) avoiding partition with the rest of the network. In general, when a node finds that it is being jammed, it starts moving out of the jammed region; at the same time it executes a detection algorithm trying to stay connected with its previous neighbors. If the evading node blindly moves away from the jammed area, the connectivity of the network could be considerably affected.

Fighting Reservation Based DoS Attacks: An opponent can only send an Request To Send (RTS) packet, requesting the medium for a time of M slots, while it does not have actual data to send. This results in the underutilization of the medium; there is no packets are on the air but the legal users cannot access it. To address this attack, there is a new control packet, called Clear To Send (CTS). The Access Point(AP) can (e.g. every K slots) sense the channel from time to time to deduce if there is an ongoing transmission, as should be the case. If the medium is not busy, the AP revokes it by sending out a CTS packet [12].

Problems of Existing Works: There are some limitations of existing works like in paper [13] there is a problem of high interference in this system and false alarm causes both of our systems to use many codes that are not actually jammed. In paper [14] the system is able to detect only Reactive Jammer attack. The system should be design for detect all types of jamming attacks. In paper [15] Rationale of Frequency Hopping (FH) Pairs is used which needs "synchronization" (at multiple levels) between senders and designated receivers (synchronization of hopping sequences, time synchronization). This is difficult. That may be a major reason in opposition to the usage of FH radios in multi-hop wireless networks. In paper [16] transmitting node do not know whether the transmission attempt was successful or not when its transmission was performed over a control-channel. For this reason, the node must repeat such a transmission for many times. Hence cluster nodes may receive multiple copies of the same control packet which may cause coincide on slots other than the control channel slots and inclusion of the same sequence number on the copies of the same packet. In paper [17] LSQ-based algorithm is proposed, in this algorithm as standard deviation increases, the performance of adaptive LSQ-based algorithm decreases. This is caused by the rising degrees of the hearing range's irregularity.

Literature Review

Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks: In this paper the authors discussed about the problem related to Cross-Layer Jamming in Wireless Broadcast Networks. In this paper the author proposed a protocol for Detection and Mitigation of Cross-Layer Jamming which allows a broadcast communication system to dynamically change the spreading codes which are used by subsets of receivers in order that some benign users can share a single spreading code, by this means conserving the number of spreading codes used at the same time. Authors show a lower bound on the number of spreading codes used concurrently to facilitate mitigate jamming by relying only on keying and not other physical characteristics. The Packet Delivery Ratio (PDR) is increased in this system. There is a problem of high interference in this System and false alarm causes both of our systems to use many codes that are not actually jammed.

Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution: In this paper the authors discussed about the problem related to Jamming Attacks in Wireless Ad Hoc Networks. The authors have proposed a new model which is based on the measure of correlation among the error and the correct reception times with the purpose of identify the presence of jamming attack in ad hoc networks. In this model a transmission node measure the Error Probability (EP) and the Correlation Coefficient (CC). The CC is among the reception error time and the correct reception time, if the CC is larger than produced relative EP then the network is

recognized as jammed. Jamming attack detection probability of this system is very high. This system shows that the Error Probability of the jammed network is equal to the Error Probability of the normal network. This system is able to detect only Reactive Jammer attack. The system should be design for detect all types of jamming attacks.

Wormhole-Based Anti-Jamming Techniques in Sensor Networks: In this paper the authors discussed about the problem related to Jamming Attack in Wireless Sensor Networks. The authors have developed suitable mathematical models for the solutions based on wired and frequency hopping pairs and it have measure the probability of success. It is a wormhole based defense mechanisms. In Rationale of Frequency Hopping (FH) Pairs there is need for "synchronization" between senders and designated receivers. That may be a major reason in opposition to the usage of FH radios in multi hop wireless sensor networks.

Thwarting Control-Channel Jamming Attacks from Inside Jammers: A control-channel jamming attack from insider nodes is discussed in this paper. The authors proposed a randomized distributed scheme for maintaining and set up a broadcast channel using frequency hopping. In this method communicating nodes are not synchronized to the same hopping sequence. As a substitute, each node follows a unique hopping sequence. Authors further proposed a mechanism for adjusting hopping sequences to dynamic spectrum conditions with no incurring any extra overhead. Evasion Delay is increased, Evasion Entropy and Evasion Ratio is also discussed in this paper. Control channel throughput is increased due to the reduction in interference between such neighborhoods. In this system transmitting node do not know whether the transmission attempt was successful or not when its transmission was performed over a control-channel. For this reason, the node must repeat such a transmission for many times. Hence cluster nodes may receive multiple copies of the same control packet which may cause coincide on slots other than the control channel slots and inclusion of the same sequence number on the copies of the same packet.

Exploiting Jamming-Caused Neighbor Changes for Jammer Localization: In this paper the authors discussed about the problem of localizing a jammer in wireless networks. The authors proposed an LSQ-based localization algorithm that estimates the jammer's location by using the changes of neighbor nodes caused by jamming. This algorithm can localize the jammer by analyzing the neighbor list changes of multiple nodes and creating a least-squares problem. So, it works fine in the jamming scenarios where network communication is disturbed. By using this system computation cost is reduced. In this algorithm when standard deviation increases, then the performance of adaptive LSQ-based algorithm decreases. This is happen due to increasing degrees of the hearing range's irregularity.

Game Theory Based Jamming Attack Detection

Overview : In this paper, for detection of jamming attacks in MANET, a game theory based defense technique is proposed. In the proposed defense technique, initially Correlation Coefficient (CC) of two communicating nodes is measured. The CC is among the reception error time and the correct reception time. Since CC can be used to detect only reactive jamming attack, along with the CC, the Carrier Sensing Time (CST), Packet Delivery Ratio (PDR) and Signal Strength (SS) metrics are also used for jamming attack detection. By applying the game theory approach, the utility function of each node is determined based on the residual energy and aggregated throughput. By checking the above metrics, the utility function is updated with a penalty value and based on the updated utility function the jamming attack nodes are detected.

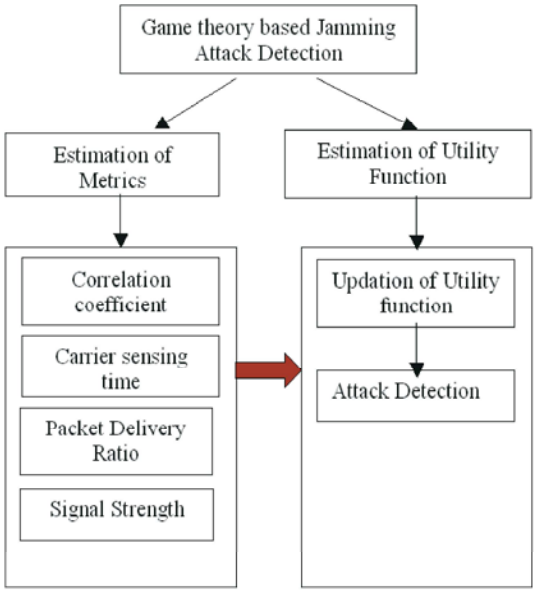

Fig. 1: Block Diagram of jamming attack detection

Basics of Game Theory: The game Z is defined as $Z = (N, S, \{UF_i\})$.

where N = finite set of players

S = action space formed as Cartesian product. i.e. $S = S_1 \times S_2 \times S_3 \times S_4 \times .. \times S_n$

UF_i = utility functions.

$UF_i = \{UF_1, UF_2, .., UF_n\}$

The outcomes are selected by a particular player i with S_i as UF_i and the particular actions selected by other players is S_{-i}. Rationality is the most basic assumption in game theory. Rational players are assumed to maximize their payoff, which is selfish motivation. In game theory, outcome is the solution of a game. Intrusion detection system (IDS) acts as one player and intruder plays as opponent player.

The main applications of game theory are as follows

- Decision making in many economic problems especially during bidding.
- Power control to set the power level of nodes. This is performed to maximize their Signal Interference to Noise Ratio (SINR), their selection of path by source node to minimize delay and their cooperation among the nodes to identify the service and forwarding of the packets to their destination.

Estimation of Metrics

Correlation Coefficient: The correlation is the link between two random variables. Thus the correlation coefficient for the transmission node between two variables P and Q is given as

$$CC = \frac{\text{cov}(P,Q)}{\sigma_p.\sigma_q} \quad (1)$$

- The value of CC is between -1 and 1
- If the value is close to 0 then it specifies absence of strong connection
- The linear relation of P and Q is given as $y = u.p + v$
- The value of u is estimated by using $\frac{\text{cov}(P,Q)}{\text{var}(P)}$

P- Reception error time

Q- Correct reception time [10]

Packet Delivery Ratio (PDR): Packet delivery Ratio is used to identify the occurrence of jamming, since the jammer can effectually debase transmissions that will leads to a very less PDR. The transmitted packets p from S_t is received at R_f. Thus from the p packets only some q packets remained distributed effectively. An effective reception is said to be only if the packets received successfully after cyclic redundancy check. Therefore PDR is defined as

$$\text{PDR} = \frac{q}{p} \quad (2)$$

where,

q- Packets received successfully after cyclic redundancy check (CRC)

p- Received packets

Signal Strength (SS): To detect natural measurement of jamming signal strength plays a significant role. Thus during the measurement the signal strength distribution may affected because of the occurrence of a jammer. Therefore by gathering enough noise level measurements during a time period prior to jamming, network devices can build a statistical model describing normal energy levels in the network. The two elementary approaches employed signal strength measurements for identifying the jamming attack.

- The first method uses either the average signal value or the total signal energy above a window of S signal strength measurements.
- The second method uses S samples to extract spectral features of the signal strength for the source of discrimination.

The average signal strength or the signal energy above a window of S samples may not reflect the datum since there may be more dissimilar received signal sample paths that may lead to the same mean or energy value. To achieve more robustness to false decisions and to improve the capacity to classify situations, it is natural to use spectral discrimination techniques to classify the signal. Thus the possible spectral discrimination mechanism is to use Higher Order Crossings i.e. HOC.

Carrier Sensing Time (CST): A jammer can prevent a legitimate source from sending out packets because the channel might appear constantly busy to the source and hence it might seem possible to use carrier sensing time as a means to determine whether a device is jammed. The carrier sensing time can be used during the resulting two circumstances are true:

- When the jammer is non-reactive or non-random,
- When the underlying MAC protocol regulates whether a channel is idle by matching the noise level with a fixed threshold.

If the above two circumstances are true, then the carrier sensing time is an efficient way to distinguish a jammed situation from an ordinary situation, such as congestion, because the sensing time will be restricted, although large, in a congested situation, but unbounded in a jammed situation.

Game Theory Based Detection: The detection phase consists of initialization and detection stages. The jammer transmits only when valid radio movement is signaled from its radio system. In order to distinguish the jamming situations, the period of error and correct reception is time is measured. Thus, this dependence measure in jamming attack situation is larger than in normal network activity. In order to measure this dependency, Correlation Coefficient is used, which is a statistic measure of relation between two random variables. Initially we assume a constant trust value for all the nodes. Each node stores the Trust Table (TT) which contains the initial trust value of the node and its neighbors.

Estimation of Utility function: The utility function at time t is computed by the following equation

$$U(t) = \delta.RE(t) + \eta.TP(t) \quad (3)$$

where
RE(t) is the residual energy measured at time t
TP(t) aggregated throughput measured at time t.
δ, η are the normalization constants.

Let Max {U(t)} and Min {U(t)} be the upper and lower bounds of the utility function, respectively.

Detection Algorithm:
Step 1:

If $CC > EP$ then
$d = d + d_1$

End if

Step 2: If $PDR > SS$ then

$d = d + d_2$

End if

Step 3: If $CST > CSThreshold$ then

$d = d + d_2$

End if

Step 4: The utility function is then updated as

$$U'(t_j) = U(t_j) - d \quad (4)$$

Step 5: For each node N_i,

If $U'(t_j) = Max\{U'(t_j)\}$

N_i is the best node

Else if $U'(t_j) >= Min\{U'(t_j)\}$

N_i is a normal node
Else if $U'(t_j) < Min\{U'(t_j)\}$
N_i is jamming attacker
End if
End for

Step 6: If N_i is a jamming attacker, then
Broadcast the warning message M [N_i, t_j] to other nodes of the network
If any node N_k, $k \neq i$, receives M, then
N_k confirms N_i as attacker
End if
End if

In step-1, the Correlation Coefficient (CC) is compared against the Error Probability (EP). If the CC is larger than produced relative EP then the penalty value is incremented by a step value of d1. In step-2, if the packet delivery ratio (PDR) is higher than the measured signal strength (SS), then the penalty function is further incremented by a step value of d2. Finally, in step-3, if the carrier sensing time (CST) is more than the carrier sensing threshold, penalty function is further incremented by a step value of d3. In step-4, the utility function is then updated by subtracting the penalty value from the current utility function. In step-5, the updated utility function of each node is checked. The nodes with maximum utility are considered as best nodes, nodes with minimum utility are considered as normal nodes whereas nodes which are having utility below the minimum utility are considered as jammed. In step-6, the details about the jamming node are broadcast to other nodes as a warning message.

Table 1: Simulation parameters

No. of Nodes	200
Area	500 X 500
MAC	802.11
Simulation Time	50 sec
Traffic Source	CBR
Rate	100Kb
Propagation	TwoRayGround
Antenna	OmniAntenna
Initial Energy	10.1J
Transmission Power	0.660
Receiving Power	0.395
No. of Attackers	2,4,6,8 and 10

Simulation Results

Simulation Parameters: We use NS-2 [17] to simulate the Theory Based Defense Technique (GTDT). In this simulation, the number of attackers is varied as 2,4,6,8 and 10. The area size is 500 meter x 500 meter square region for 50 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 1.

Performance Metrics: We evaluate performance of the new protocol mainly according to the following parameters. We compare the CCDT protocol with our proposed GTDT protocol.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average End-to-end Delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Drop: It is the number of packets dropped during the data transmission.

Residual Energy: It is the amount of energy remains in the nodes after the flow transmission.

Results & Analysis: The simulation results are presented in the next section.

Based on Attackers: In our experiment we are varying the number of attacker is varied as 2,4,6,8 and 10.

Figures 2 to 6 show the results of delay, delivery ratio, packet drop, overhead and residual energy by varying the attackers from 2 to 10 for the CBR traffic in GTDT and CCDT techniques. When comparing the

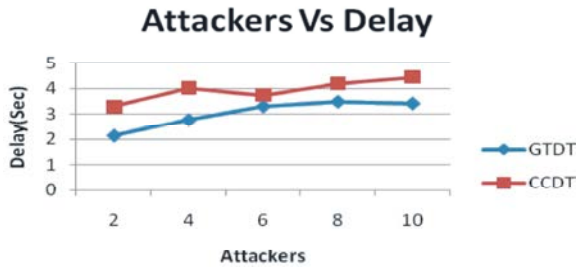

Fig. 2: Attackers Vs Delay

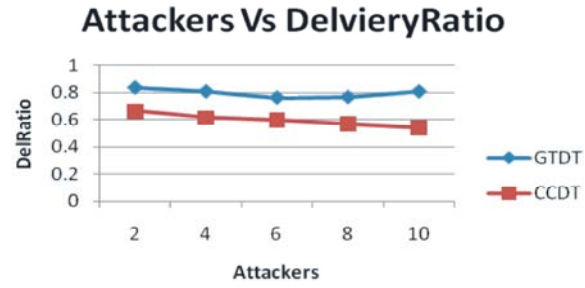

Fig. 3: Attackers Vs Delviery Ratio

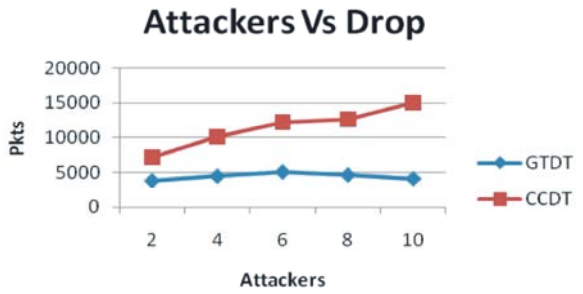

Fig. 4: Attackers Vs Drop

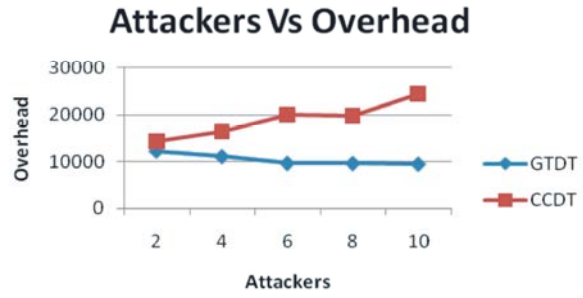

Fig. 5: Attackers Vs Overhead

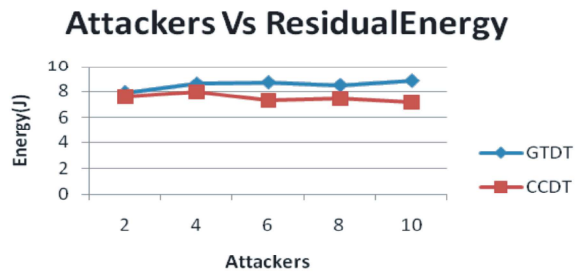

Fig. 6: Attackers Vs Residual Energy

performance of the two protocols, we infer that GTDT outperforms CCDT by 24% in terms of delay, 25% in terms of delivery ratio, 60% in terms of packet drop, 42% in terms of overhead and 11% in terms of residual energy.

CONCLUSION

In this paper, we have proposed a method to measure the correlation among the error and the correct reception times in order to detect the presence of jamming attack in ad hoc networks and also we have proposed carrier sensing time (CST), packet delivery ratio (PDR) and signal strength (SS) in order to improve the detection of jamming. Thus the method have detected specific type of jamming, in which the jammer transmits only when valid radio activity is signaled from its radio system. Therefore, the model can be able to detect the occurrence of jamming at any high range of confidence.

REFERENCES

1. Mukilan P. and Dr. A. Wah, 2012. Energy and Node Mobility based Data Replication Algorithm for MANET", IJCSI International Journal of Computer Science Issues, 9, Issue 3, No 1, May 2012 ISSN (Online): 1694-0814.
2. Aekyung Moon and Haengrae Cho, 2004. Energy-Efficient Replication Extended Database State Machine in Mobile Ad-Hoc Network, IADIS International Conference Applied Computing 2004.
3. Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos and Grammati Pantziou, 2009. A Survey on Jamming Attacks and Countermeasures in WSNs, IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, Fourth Quarter 2009. 1553-877X/09/$25.00 c 2009 IEEE.
4. Jerry T. Chiang and Yih-Chun Hu, 2010. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks, IEEE/ACM Transactions on Networking, Vol. 19, No. 1, February 2011. 1063-6692/$26.00 © 2010 IEEE
5. Alejandro Proan˜o and Loukas Lazos, 2012. Packet-Hiding Methods for Preventing Selective Jamming Attacks, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, JANUARY/FEBRUARY 2012.1545-5971/12/$31.00 2012 IEEE
6. Wenyuan Xu, Ke Ma, Wade Trappe and Yanyong Zhang, 2006. Rutgers University, Jamming Sensor Networks: Attack and Defense Strategies, IEEE Network • May/June 2006, 0890-8044/06/$20.00 © 2006 IEEE.
7. Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, 2005. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, MobiHoc'05, May 25-27, 2005, UrbanaChampaign, Illinois, USA. Copyright 2005 ACM 1595930043/05/0005 $5.00.
8. Rajani Muraleedharan and Lisa Ann Osadciw, 2006. Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System. Proc. SPIE 6248, Wireless Sensing and Processing, 62480G (May 12, 2006); doi:10.1117/12.666330
9. Murat C¸AKIRO¢GLU and Ahmet Turan ¨OZCERŸIT, 2011. Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks, Turk J Elec Eng & Comp Sci, Vol.19, No.1, 2011, cT¨UBŸITAK doi:10.3906/elk-0912-334.
10. Ali Hamieh and Jalel Ben-Othman, 2009. Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution, ANR (French Research National Agency) under CLADIS grant N. 05-SSIA-0018.978-1-4244-3435-0/09/$25.00 ©2009 IEEE
11. Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, 2011. Denial of Service Attacks in Wireless Networks: The Case of Jammers, IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, Second Quarter 2011.1553-877X/11/$25.00 c 2011 IEEE
12. Ashish Kumar, Sachin Kumar Gupta and Shubham Singh, XXXX. Packet-Hiding Methods for Preventing Selective Jamming Attacks, International Journal Of Computational Engineering Research (ijceronline.com) 3(1).
13. Mingyan Li, Iordanis Koutsopoulos and Radha Poovendran, 2010. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks, IEEE Transactions on Mobile Computing, 9(8)
14. Mario Cagalj, Srdjan Capkun and Jean-Pierre Hubaux, 2007. Wormhole-Based Antijamming Techniques in Sensor Networks Mario, IEEE Transactions on Mobile Computing, 6(1): January 2007. 1536-1233/07/$20.00 2007 IEEE

15. Sisi Liu, Loukas Lazos and Marwan Krunz, 2012. Thwarting Control-Channel Jamming Attacks from Inside Jammers, IEEE Transactions on Mobile Computing, Vol. 11, No. 9, September 2012, 1536-1233/12/$31.00 2012 IEEE
16. Zhenhua Liu, Hongbo Liu, Wenyuan Xu and Yingying Chen, 2021. Exploiting Jamming-Caused Neighbor Changes for Jammer Localization", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 3, March 2012,1045-9219/12/$31.00 2012 IEEE.
17. Network Simulator: http:///www.isi.edu/nsnam/ns.