Cryptographic Puzzles Based Data Transmission and Detecting Jamming Attacks in Wireless Networks

M. Dharani and S. Narmadha*
Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India

Keywords: Wireless Network, Puzzle Gaming Technique, Data Hiding Mechanism, Cryptographic Techniques.

Abstract: When nodes in wireless networks compete for access to a single wireless medium, collisions frequently occur. Having the destination node combine inter-nodes for data transfer when using cooperative wireless communications increases immunity to interference. One of the primary methods used to compromise the wireless environment is jamming. By blocking off providers to authorized customers, while true visitors are slowed down by means of the giant quantities of unlawful traffic, it operates. By randomly delivering unauthenticated packets to each network wireless station, the attacker can quickly compromise the network. Because wireless networks rely on shared media, it is simple for adversaries to conduct denial-of-service and jamming assaults. Using the following approaches, the jamming and denial-of-service attacks in our proposed work can be easily detected, and network performance can be enhanced. We provide a data-hiding mechanism and puzzle-gaming technique that aid in determining whether inter-nodes are jammed or not. In network transactions, cryptographic methods and data concealment are strengthened to ensure the transaction's security. The methodology can improve network throughput and server processing overhead while ensuring secure transactions.

1 INTRODUCTION

To connect participating nodes, wireless networks rely on the wireless medium's continuous availability. However, this medium is susceptible to various security threats because of its open nature. vulnerabilities. Wireless signals can be intercepted, fraudulent messages injected, and legitimate messages jammed by anybody possessing a transceiver. While cryptographic measures can prevent message injection and eavesdropping, jamming attacks are far more difficult to prevent. They have been shown to be capable of carrying out major Attacks on wireless networks that cause a denial of service (Alejandro and Loukas 2022). In the most basic jamming technique, the attacker sends a continuous jamming signal or a series of brief jamming pulses to disrupt message reception. Jamming attacks are frequently examined using a jammer is not a part of the network in an external threat model. jamming techniques, according to this paradigm, consist of transmitting high-power interference signals constantly or at random. Adopting a "always-on" technique, on the other hand, offers a number of disadvantages. The adversary must first spend a lot of energy jamming the appropriate frequency ranges. Second, because of the persistent existence of extremely high interference magnitudes (Alejandro and Loukas, 2022) this kind of assault is easy to detect. Ad hoc networks are expected to considerably improve military, industrial, and utility communications that are essential to their missions. To stop part or all victim communication, an adversary may try to target a victim's ad hoc network. In ad hoc wireless networks, Multiple degrees of research have been done on such denial-of-service (DoS) attacks (Brown 2006). DoS attacks where the attackers are users of the target ad hoc network have been studied by several researchers. Ad hoc networks are especially vulnerable to peer-based assaults since they rely on peer node cooperation to function. We examine encrypted victim networks in this study, where the attacker cannot directly affect any victim communication because headers and payload of the entire packet included—is encrypted. In this circumstance, the offender must deploy jamming, a type of external physical layer-based DoS (Brown, 2006).

* Assistant Professor

Dharani, M. and Narmadha, S.
Cryptographic Puzzles Based Data Transmission and Detecting Jamming Attacks in Wireless Networks.
DOI: 10.5220/0012611400003739

In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 216-220
ISBN: 978-989-758-661-3

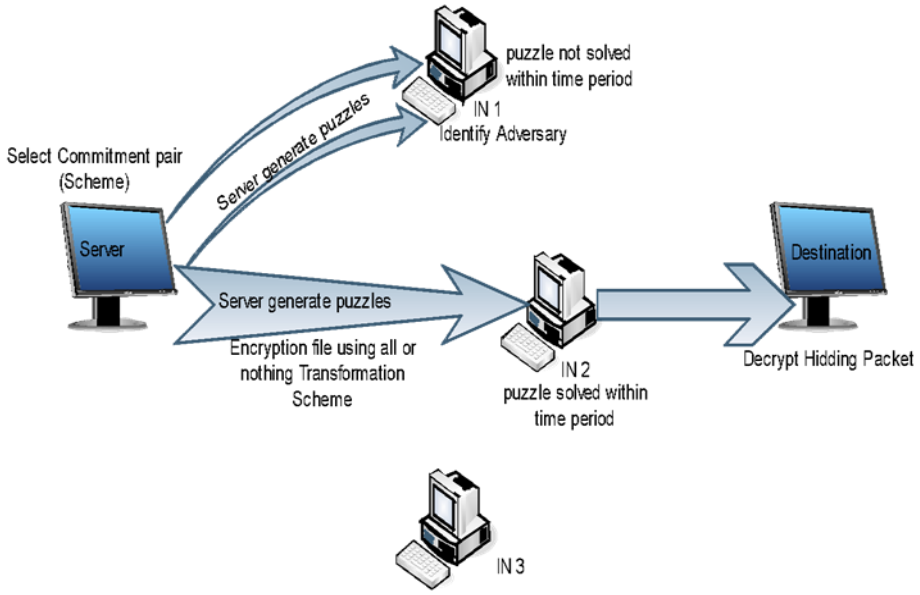

Figure 1: System Architecture.

2 RELATED WORK

2.1 Encrypted Wireless Ad Hoc Network Jamming and Sensing

The challenge of an attacker jamming a wi-fi ad hoc community of an encrypted sufferer is examined in this paper. When dissecting jamming into its component parts, this article focuses on the layer of the transport/network (Brown 2006). A layer that is clogged, which takes advantage of the When AODV and TCP can identify the victim packet types, they have been demonstrated to be quite effective in both simulated and real networks. However, it is anticipated that encryption will hide the complete header and package content, leaving the attacker with only the capacity to detect packet size, timing, and sequence. The development and testing of a sensor using real-time data. The designation has been proven to be quite dependable for a variety of unusual packet types. The implications for improving community safety are investigated in conjunction with the proportionate contributions of size, time, and sequencing.

2.2 Methods for Hiding Packets to Prevent

The Wi-Fi medium's openness makes it inclined to deliberate interference attacks, occasionally acknowledged as jamming. This deliberate disruption of Wi-Fi communications can be exploited as a springboard for Denial-of-Service assaults in opposition to Wi-Fi networks. Jamming has frequently been dealt with the usage of an exterior hazard model. Nevertheless, attackers that are privy to network and protocol specifications can carry out low-effort jamming attacks that are challenging to find and defend against. That is research (Alejandro and Loukas 2022) we investigate the topic of concentrated attacks on WiFi networks that jam traffic. In these assaults, the enemy selectively targets high-value messages while being active for a brief period of time. We demonstrate the advantages of selective jamming in terms of community performance degradation and adversary effort by offering two case studies, one on TCP and one on routing (Alejandro and Loukas 2022). We show that physical layer classification of packets in real-time enables the launch of targeted jamming assaults. To address We create three methods that combine physical-layer cryptography with cryptographic primitives to defend against these assaults. characteristics. We test the computational and verbal exchange price of our techniques and monitor their security (Alejandro and Loukas 2022).

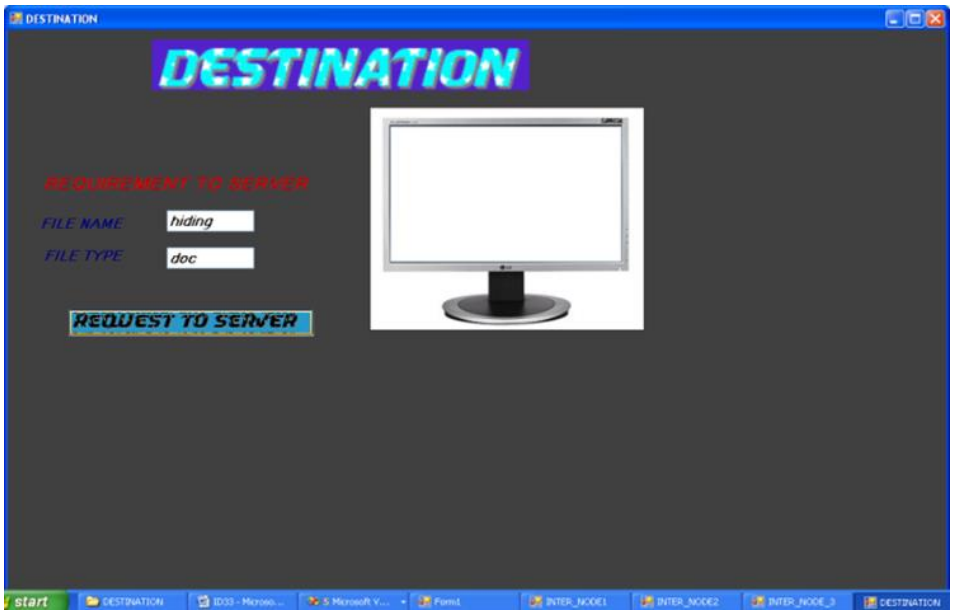

Figure 2: Destination Node.

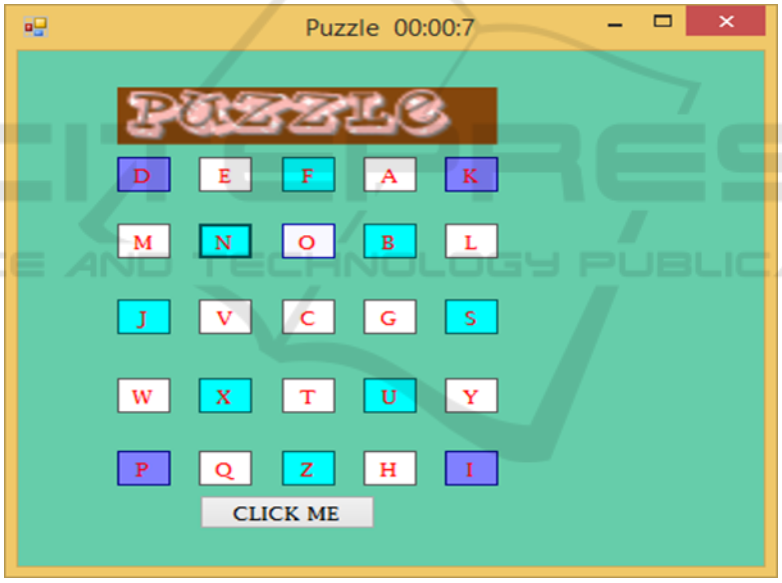

Figure 3: Solves the challenge and transmits information to the target.

2.3 Attacks on Control-Channel Jamming in Multi-Channel Ad Hoc Networks Mitigation

In multi-channel ad hoc networks, the issue of control-channel jamming assaults is covered. As opposed to the conventional viewpoint, which considers We think of jammer assaults as a physical-layer weakness and a modern adversary who takes use of their understanding of protocol mechanics as well as cryptographic portions extrapolated from infected nodes in order to increase the impact of his attack on higher-layer features (Liu et al 2007, Merkle 1978). We suggest fresh security metrics that gauge an adversary's capacity to prevent entrance to the manipulated channel as well as the total amount of time required to re-establish the manipulated channel. Additionally, we suggest a distributed, randomised device that permits frequency hopping by nodes to create extra control channels (Liu et al 2007). Our strategy minimizes the outcomes of node compromise due to the fact no two nodes use the identical hopping

Figure 4: Server- An example of a server sending a packet across an inter node.

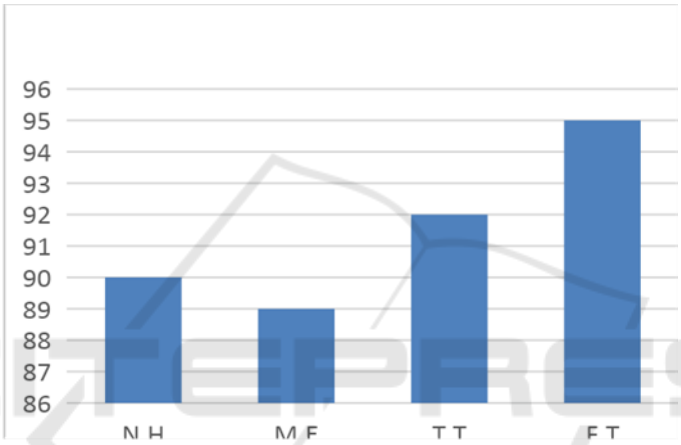

Figure 5: Average route discovery time (non-congested network).

sequence, making it a traditional type of frequency hopping. A compromised node is additionally recognized in my opinion through its hop sequence, which isolates it from any upcoming know-how about the manipulate channel's frequency role (Liu et al 2007).

3 PROBLEM DEFINITION

To connect participating nodes, wireless networks rely on the wireless medium's continuous availability. However, this medium is susceptible to various security threats because of its open nature. vulnerabilities. Wireless signals can be intercepted, fraudulent messages injected, and legitimate messages jammed by anybody possessing a transceiver. Cryptographic techniques can be employed to prevent message injection and eavesdropping, but jamming attacks are much more difficult to prevent (Alejandro and Loukas 2022). They have been shown to be capable of carrying out major Attacks on wireless networks that cause a denial of service. The adversary sends a continuous jamming signal or a series of brief jamming pulses to obstruct message reception in the most basic jamming. Jamming assaults are regularly analyzed the usage of an exterior chance mannequin the place the jammer is no longer a element of the network. This mannequin consists of the transmission of high-power interference indicators always or at random as one of the jamming techniques. Adopting a "always-on" strategy, however, has a number of drawbacks. The enemy must first use a large energy required to jam the appropriate frequency ranges. Second, this kind of attack is simple to spot due to the persistent presence of exceptionally high interference levels.

4 PROPOSED MODEL

In this study, the issue of jamming is addressed using the internal threat model. We take into account a educated opponent who is conscious of community

secrets and techniques and the specifics of how community protocols are applied at any layer in the community stack. In order to launch selective jamming assaults that target only particular communications of "high value," the enemy uses his insider information. A jammer may, for example, target TCP acknowledgments to severely limit an end-to-end flow's throughput or Routing layer route-request/route-reply messages to thwart route discovery. The enemy must be able to deploy specific jamming attacks in order to able to execute a "classify-then-jam" technique prior to the end of an electronic gearbox. Such a technique can put into practice by decoding packets as they are sent or by utilizing protocol semantics to categories transmitted packets. Selective jamming necessitates a thorough understanding both the specifics of the physical (PHY) layer and those of higher levels. We created three strategies that, by obstructing real-time packet classification, turn an intentional jammer becomes an accidental one. Our structures combine physical-layer houses with cryptographic primitives like dedication schemes, cryptographic riddles, and transformations that are all-or-nothing (Alejandro and Loukas 2022).

In the first series of experiments, we used a multihop route to connect a client and a server for a single file transfer. The client asked the server for a 5KB file. We measured the actual throughput of the TCP connection in the following situations to investigate the impacts of packet concealment: There is no message encryption or packet concealment (N.H. (M.E.), transmission time (T.T.), and file transfer (F.T.). Because there is no cross-traffic, the relatively little communication justifies the overhead of each concealing technique as well as the minimal queuing delay at intermediate routers. Cryptographic challenges are sometimes exploited in hiding methods. Figure.2 shows a destination node that receives the file via inter-node communication from the server and that node that solves the puzzle

5 CONCLUSIONS

In wireless networks, the issue of targeted jamming assaults has been solved. Because the jammer is a member of the community being attacked, it is informed of the protocol requirements and shared community secrets and practices. This is a paradigm of internal opponents. We proved the jammer's capability categorize sent real-time packets by deciphering the initial scant signs of a continuous transmission. We investigated how targeted Jamming attacks had an impact on routing and TCP, among other network protocols. (Alejandro and Loukas 2022). Our research demonstrates that a specific jammer can have a significant detrimental impact on performance with little effort. We devised three ways for converting a targeted jammer into an arbitrary one by impeding instant packet categorization. Physical-layer features are mixed with cryptographic fundamentals like all-or-nothing transformations, cryptographic riddles, and commitment schemes in our systems. We assessed the safety of our techniques and calculated the overhead for computation and communication.

REFERENCES

T. X. Brown, J. E. James, and A. Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

Alejandro Proan˜o and Loukas Lazos “Packet-Hiding Methods for Preventing Selective Jamming Attacks” IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/february 2022.

L. Lazos, S. Liu, and M. Krunz, “Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks,” Proc. Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.

X. Liu, G. Noubir, and R. Sundaram, “Spread: Foiling Smart Jammers Using Multi-Layer Agility,” Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

Y. Liu, P. Ning, H. Dai, and A. Liu, “Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication,” Proc. IEEE INFOCOM, 2010.

R. C. Merkle, “Secure Communications over Insecure Channels,” Comm. ACM, vol. 21, no. 4, pp. 294-299, 1978.