DoS Attack Prevention using CPHS and SHCS Algorithms

Lakshmi Narayan B.N.
Department of Master of Computer Applications,
NitteMeenakshi Institute of Technology,
Yelahanka, Bengaluru, Karnataka

Mariyan Richard A.
Department of Master of Computer Applications,
NitteMeenakshi Institute of Technology,
Yelahanka, Bengaluru, Karnataka

Prasad Naik Hamsavath, PhD
Department of Master of Computer Applications,
Nitte Meenakshi Institute of Technology,
Yelahanka, Bengaluru, Karnataka

ABSTRACT
In the present world, transmission of data through wireless networks is an upcoming trend. Since wireless networks are prone to intendedintrusion attacks, the transmission leads to congestion in the network. The familiar attack that is faced during the transmission of data is Denial-of-Service (DoS) attack. This kind of attack is intended to render a machine or resource in the network unavailable to the target users to momentarily or indefinitely disrupt or suspend services of a host that is connected to the Internet.Typically,the external threat model addresses jamming. Yet, opponentswho possess the network secrets and are aware of the protocols can deliver efficient and guarantedto. In this paper, we propose to implement a Cryptographic Puzzle Hiding Scheme (CPHS) and Strong Hiding Commitment Scheme (SHCS) to prevent DoS attacks.

Keywords
Cryptographic Puzzle Hiding Scheme (CPHS), Strong Hiding Commitment Scheme (SHCS), DoS Attack.

1. INTRODUCTION
The open nature of the wireless network leads to vulnerability in security threats eavesdropping and injection of a message in a network can be avoided using recent techonologies like cryptographic methods. Since jamming attacks are harder to counter, they show severe DoS attacks against wireless networks [6].A DoS attack is an attack with the objective of not letting the intended users use the required network resources like a web service, a website, or a computer system. The broadcast channel is the wireless communication medium that exposes the physical layer of the communication to jamming [7].

This paper attempts to deal with the problem of DoS attackswith an internal threat model. An opponent who is aware of the network secrets and implementation details is considered. The opponent launches a jamming attack in which specific data istargeted by using the internal knowledge on the network[2].

2. PROBLEM STATEMENT
Consider the scenario as shown in Figure 1, where Node *A* and Node *B* communicate via a wireless network. Between the communication of both Node *A* and Node *B*, there is a jammer Node *J*. When Node *A* transmits data *m*to Node *B*, Node *J* blocks the data *m* or drops the data *m*, due to which Node *B* will not receive the data *m*. We address the problem of blocking the data using jammer *J*, which is a DoS attack [1].

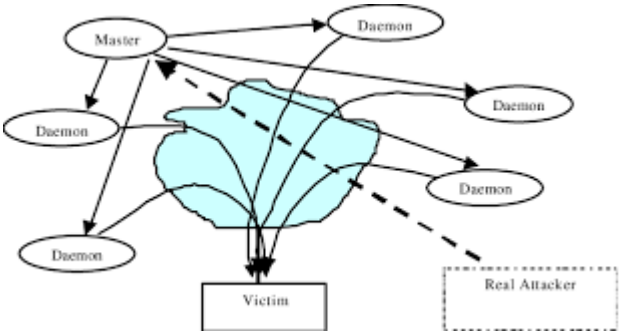

Figure 1: Realization of DoS attack

3. RELATED WORK
LoukasLazoset is proposing a randomised distributed mechanism that allows nodes to create a new control channel using frequency hopping [5]. The proposed method differs from classic frequency hopping wherein the same hopping sequence is shared by no two nodes. This justifies the impact of node compromise. Additionally, a hop sequence distinctly identifies the compromised node which leads to its two way isolated individual paths.

4. PROPOSED SYSTEM
The DoS assault issue under the internal danger model has been taken into account. An opponent who is aware of network secrets, internal functioning of the network and network protocols are responsible for the design. The attacker is mainly concerned with extremely important and sensitivedata[3].

The proposed system uses two algorithms, CPHS and SHCS for the secured transmission of data through the wireless network. The sender can choose either of the two algorithms for the transmission of the data.

5. IMPLEMENTATION
In this section, we describe how CPHS and SHCS algorithms work.

5.1 Cryptographic Puzzle Hiding Scheme (CPHS)
In this section, a packet hiding method is presented which is mainly based on cryptographic puzzles. The thought behind the creation of puzzles is to compel the user of puzzle to execute a pre-defined set of computation before he extorts the internet secrets. Since, the time required for solving the puzzle is harder and has computational procedure, the attacker cannot easily extract the data.

(C,P), where $C = E_k(\pi_1(m))$. At the receivers' end, receiver *R*

solves received puzzle *P'* to recover key *k'* and computes $m' = \pi^{-1}(D_{k'}(C'))$. If $m' = m$, the receiver accepts *m'* else discards *m'*.

InFigure 2, the sender transmits the data by choosing the CPHS algorithm option. At the sender side, sender will be asked for the creation of puzzle and he will also be asked for specifying the timestamp, within which the puzzle has to be solved by the receiver[4].

As shown in the Figure 3, if the attacker tries toblockthe data which is sent by the sender, the intruder will get a message - "*Can't block encrypted message*".

In receiver side, as shown in the Figure 4, when the message is received the receiver will be asked for solving the puzzle. If the receiver solves the puzzle within the timestamp the data will be displayed to the receiver else it will be discarded. Figure 5 shows the received data at the sender side.

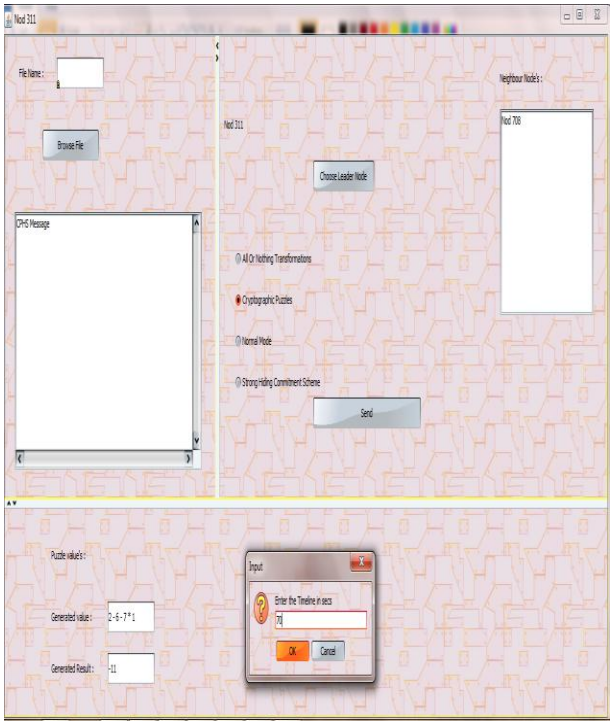

Figure 2: Sending Message at Sender Side(CPHS)

5.2 Strong Hiding Commitment Scheme(SHCS)

Here, we present a system for packet hiding that is based on commitments. A commitment scheme is a two-phase dynamic protocol that follows the basic properties of hiding and binding.

Let sender *S* have a packet *m* for transmission. *S* constructs (C,d) = commit(m) where $C = E_k(\pi_1(m))$, $d = k.E_k$is the commitment function and encryption algorithm, $k \in \{0,1\}^s$ is a randomly selected key. The sender broadcast $(C \,||\, d)$, where "||" denotes concatenation operation.At receiver side, receiver *R* computes $m' = \pi^{-1}(D_{k'}(C'))$. If $m' = m$, the receiver accepts *m'* else discards *m'*.

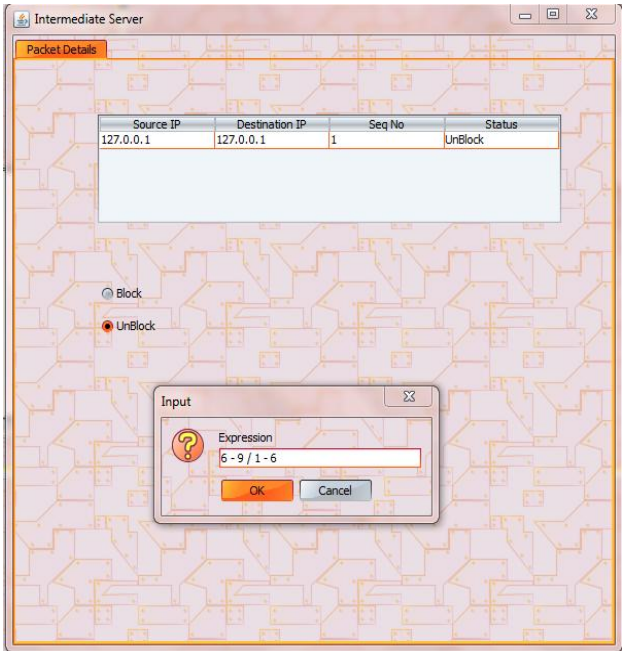

Figure 3: Receiver is asked to solve the puzzle

Consider the Figure 5, the sender transmits the data by choosing the SHCS algorithm option. At the sender side, sender will be asked for the secret key which will be shared with the receiver.

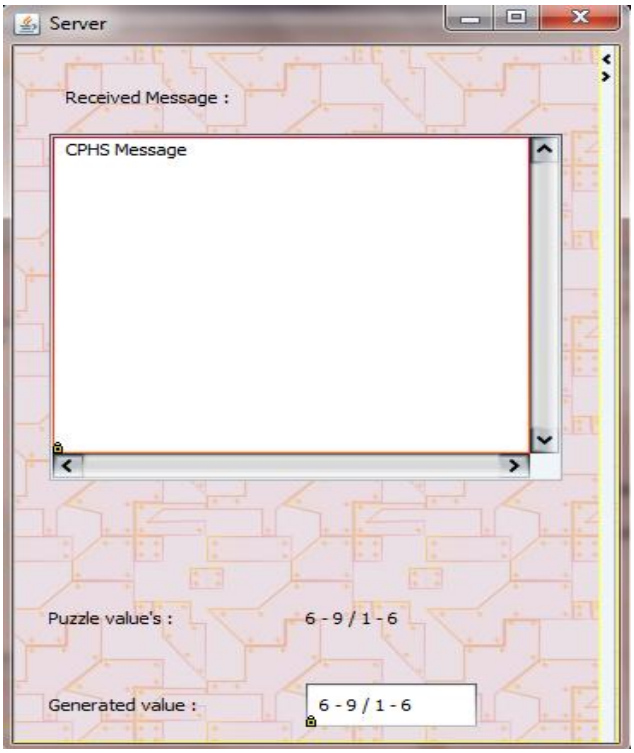

Figure 4: Received Message at Receiver Side

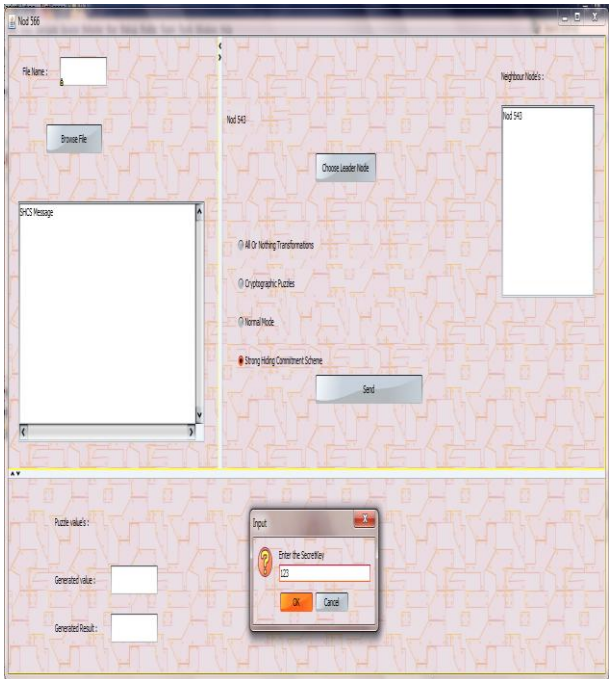

Figure 5: Sending Message at Sender Side(SHCS)

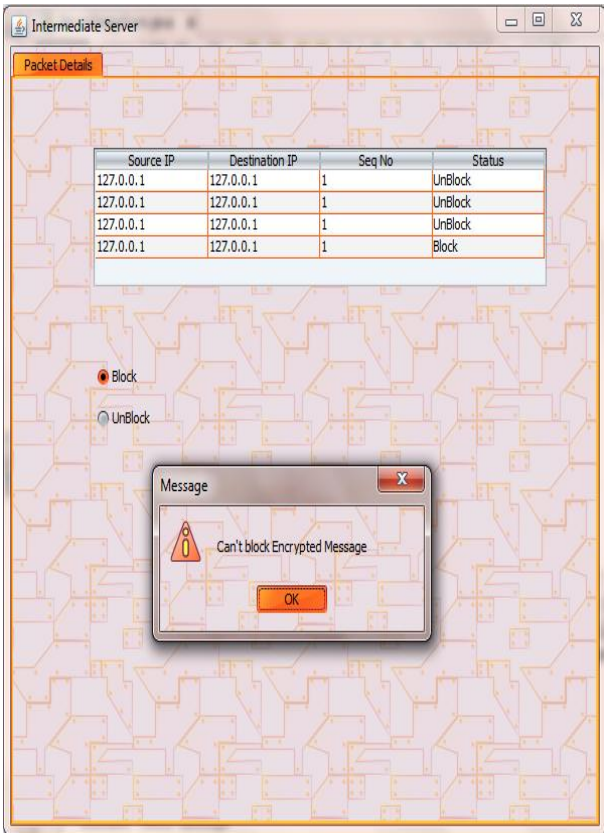

Figure 6: Message shown at Intermediate Server

As shown in Figure6, if the attacker tries to block the data which is sent by the sender, the intruder will get a message as "Can't block encrypted message" [7].

In the receiver side, as shown in Figure 8, when the message is received the receiver will be asked for the secret key. If the receiver gives the correct secret key (Figure 7), the data will be displayed to the receiver else it will be discarded [8].

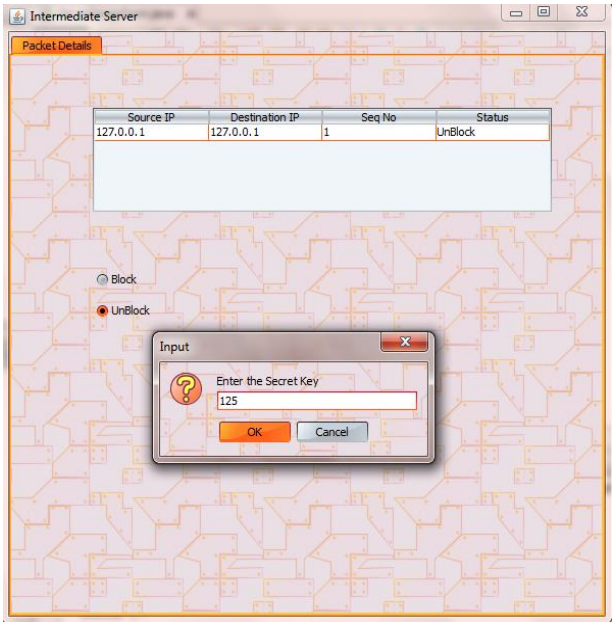

Figure 7: Receiver is asked for the secret key

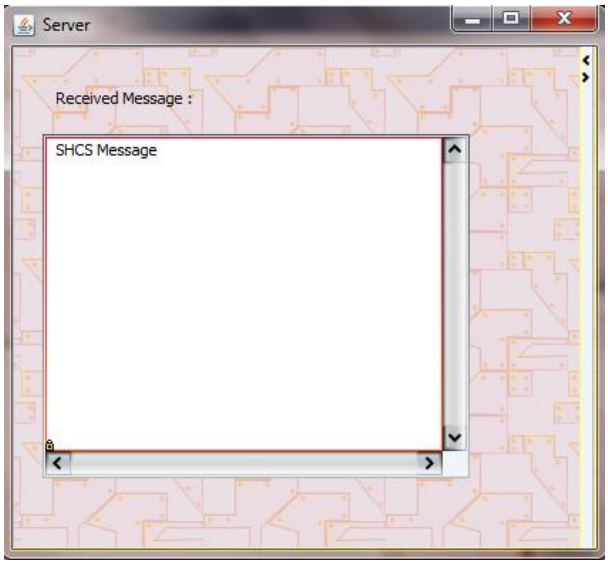

Figure 8: Received Message at Receiver Side

6. CONCLUSION

The topic of DoS attacks on wireless networks was discussed in this report. The internal adversary paradigm in which the attacker is a member of the network is quickly considered. We have implemented CPHS and SHCS algorithms to solve the DoS attack problem. The CPHS algorithm uses the cryptographic puzzle hiding mechanism to solve the mentioned problem and the SHCS algorithm uses the commitment scheme to solve the problem [9].

7. REFERENCES

[1] Alejandro Prono and LoukasLazos. Packet-Hiding Methods for Preventing Selective Jamming Attacks. In *IEEE ICC* Conference, 2010.

[2] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing ofencrypted wireless ad hoc networks. In *Proceedings of MobiHoc*, pages120–130, 2006.

[3] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijammingtechniques in sensor networks. *IEEE*

Transactions on MobileComputing, 6(1):100–114, 2007.

[4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, andP. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. *ACMTransactions on Sensors Networks*, 5(1):1–38, 2009.

[5] P. Tague, M. Li, and R. Poovendran. Mitigation of control channeljamming under node capture attacks. *IEEE Transactions on MobileComputing*, 8(9):1221–1234, 2009.

[6] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *ProceedingsofMobiHoc*, pages 46–57, 2005.

[7] Yongjun Zhao, Sherman S. M. Chow. "Updatable Block-Level Message-Locked Encryption". Published in: IEEE Transactions on Dependable and SecureComputing.DOI: 10.1109/TDSC.2019.2922403 Publisher: IEEE. Date of Publication: 12 June 2019.

[8] Xingyuan Wang, SuoGao."Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network".Published in : ELSEVIER, Information Sciences. Volume 539, October 2020, Pages 195-214.

[9] Chin-Chen Chang, Guo-Dong Su, Chia-Chen Lin. "An improved Sudoku-based data hiding scheme using greedy method".Published online 22 September-2020. https://doi.org/10.1504/IJCSE.2020.110177.