# Protocol Analysis to Prevent Storm Attacks In 3G Mobile Networks

**B. Radhika[1] V. Vetriselvi[2] J. Sengottuvelu[3]**
[2]Assistant Professor
[2]Department of Information Technology & Applications
[1,2]Shrimati Indira Gandhi College, Tiruchirapalli [3]Value Tech

*Abstract*— The advent of mobile smart phones has led to a surge in numerous applications with a lot of network traffic. This in turn leads to signal storm attacks from malicious users, who disrupt the system by creating signaling storms. Malware attacks are quickly becoming a major security concern due to the advent of smart mobile devices and the increasing capacity and use of mobile networks for Internet access. The increasing number of host mobile malware adds to the problem. The infected devices cause a cascading effect creating signaling and network disruptions both deliberately and also due to malicious attacks. A signaling storm is one where the users are denied service by making huge attacks on the resources of the system either directly or indirectly taking control of other nodes in the network and sending huge amounts of request signals. This causes flooding, identity problems, injection attacks etc. The purpose is to detect such signaling storms in the first place. Next using the proposed hybrid Radio Resource protocol such attacks should be blocked and the malicious node should be removed from the network. The revocation will show sufficient congestion relief in the network traffic.

***Key words:*** 3G Storm Attacks, Mobile Computing, Signal Storms

## I. INTRODUCTION

A signal storm attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware, or bypass access controls. There are several different types of random and specific signal storm attacks. Mostly malicious parties use this to accomplish their hidden agenda of disrupting the network. Disruption includes include IP address storm attacks, ARP storm attacks, and DNS server storm attacks. 3G signal storm is when an attacker pretends to be someone else in order to access restricted resources and steal vital identities as well. Such impersonation attacks can take a variety of different forms; for instance, an attacker can impersonate a genuine user by using the Internet Protocol (IP) address and then hack into their personal accounts. Also, an attacker may send fraudulent signals from different IP addresses to order to capture users' login names, passwords, and account information, which are called identity attacks. Faking an email or website is sometimes called a phishing attack. Another type of 3G signal storm involves setting up a fake wireless access point and tricking victims into connecting to them through the illegitimate connection. The problem here is to detect such attacks sandbox them and then revoke such malicious users.

## II. RELATED WORK

Studies on signalling attacks include the SMS flooding attack by W. Enck et al [1] show that an SMS attack originating from GSM capable Internet hosts significantly degrades and may also prevent voice and SMS services on the cellular network. P.Traynor et al [2] proposed novel countermeasures for SMS based server signal attacks. In their work SMS of death: From analyzing to attacking mobile phones on a large scale[3] C. Mulliner et al show the possibility of SMS attacks in feature phone itself where they originate from within the host cellular network. Serror et al. [4] used CDMA networks to prove that such networks exhibits a sharp rather than a graceful degradation under load. Such problems exist in 4G networks as well and have been the research of R. Bassil et al[5]. RRC-based signalling storm attacks have been researched by P. P. Lee et al [6], where the authors do a remote host attack on UMTS networks and also provided solutions which are online based statistical cumulative sum tests. R. Bassil [7] et al evaluate the effect of an RRC-based storm signalling attack on an LTE network. But they used simulation and showed resulting considerable performance degradation in the LTE network. Z. Zhang et al [8] studied the utilization of LTE radio channels such as PUSCH and PUCCH due to keep-alive messages, which are a considerable source of signalling problems. F. Ricciato et al [9] studied in detail 3G signalling attacks and have identified the system decisions that result in such attacks, wherein they proposed randomization of the radio resource management (RRM) and mobility management (MM) procedures. Wu et al. [10] proposed the randomization of the RRM method in 3G networks, and proved to an extent that certain attacks can be blocked while degrading performance slightly.

## III. 3G STORM ATTACKS

The signal storm attacks can broadly be classified into the following headings where a storm causes any of the following damages to the server or servers or to the network itself as a whole. In the implementation phase all the signal storm attacks in the different layers are controlled.

### *A. Code Injection*

In this type of attack the intruder injects the code into a batch file and then embeds it in the server without its knowledge. This code then starts executing automatically to start different programs in the server. So the server unknown to itself responds to the intruder's requests and various programs hog a lot of the memory space. This causes immense strain to the server and ultimately it buckles under the pressure. Finally the server succumbs to the pressure and the intruder has the upper hand. The adversary blocks the started program from the server. Code injection also causes false data to be given as parameters to the started programs which are in the self-executable batch files. This causes the programs to crash in the future.

### *B. Identity Attacks*

Here the intruders' purpose is to steal the data from the server using masquerading techniques. The data may range from ordinary files to system files, user sensitive transaction data and also passwords. All the retrieved data will be

 

misused causing huge losses to both the integrity of the data server as well as the users of the server.

### *C. Ping Attack*

In this signal storm attack the attacker tries to crash the server. This is done by rebooting it or killing a large number of server systems by constantly pinging the server. During this pinging no process will work in the server and so it will be a storm of a kind that disrupts all processes. All this ping based storm attack happens from a remote machine. This is a very serious issue because if not detected it multiplies rapidly and destroys all the incoming requests and responses.

### *D. Flood Attack*

The flood attack in storm signals as the name implies creates a flood of DDOS requests or other awkward requests in such a manner that it crumbles and cripples the network. A small sample would be to flood the cache with dummy data files so that the storage is drastically reduced. Based on the speed flood attacks cause severe damage to the server and before it is detected the clients may leave you. Sometimes flooding causes network disruptions also. The attack is a designed in such a manner as if a diagnostic check is being done. So there is no suspicion.

### *E. Detection Module*

This is the place where the hybrid detection algorithm if it notices any discrepancy as such raises an alarm. It might be due to a flood, code injection, identity, or ping etc. Once the alarm is raised all flags are automatically alerted and the detection alarm goes on. Next the action has to be stopped. Here all the henceforth actions are sandboxed and then the alarm algorithm goes into stealth mode to find the intruder. All requests are flagged off and thus any untoward storm signal attacks are detected. The next phase is the most important one where actions are induced to catch the intruder and punish the intruder. All activities are automatically logged for future references. Fine tuning the detections classifies the type of signal storm attack and thus responses are based on that tuning signal received.

### *F. Revocation*

Finally the last phase after detection takes place. It is known as the process of intruder or attacker revocation. After sandboxing the anomalous – bad actions successfully, it is most important to catch the signal storm attacker, failing which the attacker will cause more trouble and push the server into damage control mode. This module tackles this issue successfully and traces the route of the attack by following the return response in stealth mode unknown to attacker and then unmasks them so that they are immobilized and unable to cause further attacks.

## IV. PERFORMANCE EVALUATION

The results of the model have been evaluated and found that with respect to the various signal storm attacks the model is resilient and detects with accuracy when compared with other existing models presented in related works. The findings have been tabulated and then appropriate graphs have been drawn to show the results.

| Models | Attack Type 1 | Attack Type 2 | Attack Type 3 | Attack Type 4 |
|---|---|---|---|---|
| Proposed | 98.62% | 97.40% | 29.60% | 86.33% |
| Others | 92.21% | 96.80% | 16% | 60% |

Table 1: Showing Attacks Detection Comparison

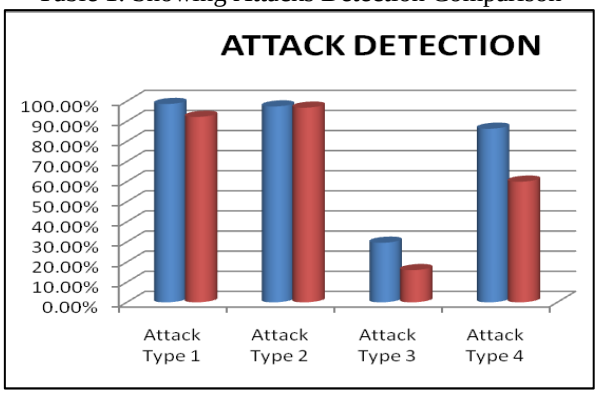


Fig. 1: Chart Showing Attack Detection Rates

As you can clearly see that the 3G signal storm method approach fares better in terms of detecting all types of attacks rather than non-layered types on standard testing times. Further it is also observed that the 3G signal storm is most effective in the attack traffic to the initial layers in the system.

### *A. False Alarm Rates*

| IDS METHOD | False Positive | False Negative |
|---|---|---|
| Proposed | 0.91 | 0.07 |
| Other Methods | 0.6 | 0.3 |

Table 2: Showing Alarm Rates

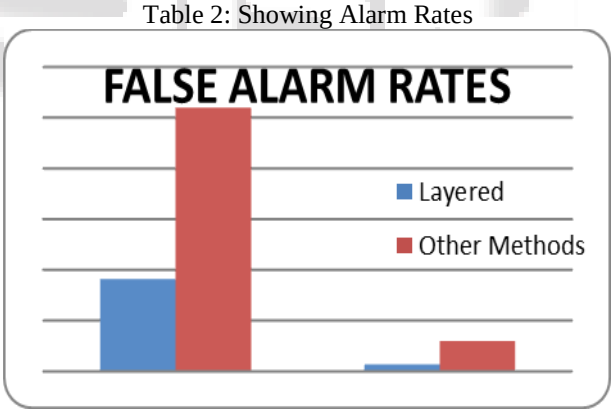


Fig. 2: Chart Showing False Alarm Rates

As shown above false alarm rates like false positive i.e. showing an 3G STORM attacker when there is none and false negative i.e. allowing an intruder as a genuine person without detection is significantly lower when compared with other Methods methods in 3G STORM Approach.

## V. CONCLUSION

Thus the 3G signal storm attacks are prevented successfully. All the four layers of attacks like injection, identity, denial of service, DOS, flooding, pinging etc. The unique physical property associated with each wireless is used and used for detecting such types of attacks called signal storms. The proposed model are accurate in localizing the attacking nodes and also effective in neutralizing them and also has the least false alarm rates with less overheads. The proposed

approach can both detect the presence of attacks as well as determine multiple adversaries simultaneously. In this model it is possible to eliminate any number of storm attacks. The model has been tested to achieve better accuracy of determining the number of signal storm attackers than other methods under study.

In future the attacks detection model may be adapted to other network strategies which include other network models apart from wireless networks. Such networks will enhance the security and prevent other related attacks and prevent collateral damages to the system.

## REFERENCES

[1] W. Enck, P. Traynor, P. McDaniel, and T. L. Porta, "Exploiting open functionality in SMS-capable cellular networks," in Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05), Nov. 2005

[2] P. Traynor, W. Enck, P. McDaniel, and T. L. Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," IEEE/ACM Trans. Networking, vol. 17, no. 1

[3] C. Mulliner, N. Golde, and J.-P. Seifert, "SMS of death: From analyzing to attacking mobile phones on a large scale," in Proc. 20th USENIX Conf. on Security (SEC'11), Aug. 2011

[4] J.Serror, H.Zang, and J.C.Bolot, "Impact of paging channel overloads or attacks on a cellular network," in Proc. 5th ACM W'shop on Wireless Security (WiSe'06), Sep. 2006

[5] A. Baraev, U. Ayesta, I. M. Verloop, D. Miorandi, and I. Chlamtac, "Technical vulnerability of the E-UTRAN paging mechanism," in Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC'12), Apr. 2012

[6] P. P. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," Computer Networks, vol. 53, no. 15, pp. 2601–2616, Oct. 2009

[7] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, "Effects of signaling attacks on LTE networks," in Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA'13), Mar. 2013

[8] Z. Zhang, Z. Zhao, H. Guan, D. Miao, and Z. Tan, "Study of signaling overhead caused by keep-alive messages in LTE network, in Proceedings of the 78th IEEE Vehicular Technology Conference (VTC Fall'13), Sep. 2013

[9] F. Ricciato, A. Coluccia, and A. DAlconzo, "A review of DoS attack models for 3G cellular networks from a system-design perspective," Computer Communications, vol. 33, no. 5, pp. 551–558, Mar. 2010.

[10] Z. Wu, X. Zhou, and F. Yang, "Defending against DoS attacks on 3G cellular networks via randomization method," in Proceedings of the 2010 International Conference on Educational and Information Technology (ICEIT'10), Sep. 2010

 