Optimization of Recent Attacks Using Internet Protocol

A. Rengarajan, C. Jayakumar, R. Sugumar

Abstract— The Internet threat monitoring (ITM) systems have been deployed to detect widespread attacks on the Internet in recent years. However, the effectiveness of ITM systems critically depends on the confidentiality of the location of their monitors. If adversaries learn the monitor locations of an ITM system, they can bypass the monitors and focus on the uncovered IP address space without being detected. In this paper, we study a new class of attacks, the invisible LOCalization (iLOC) attack. The iLOC attack can accurately and invisibly localize monitors of ITM systems. In the iLOC attack, the attacker launches low-rate port-scan traffic, encoded with a selected pseudo noise code (PN-code), to targeted networks. While the secret PN-code is invisible to others, the attacker can accurately determine the existence of monitors in the targeted networks based on whether the PN-code is embedded in the report data queried from the data center of the ITM system. We formally analyze the impact of various parameters on attack effectiveness. We implement the iLOC attack and conduct the performance evaluation on a real-world ITM system to demonstrate the possibility of such attacks. We also conduct extensive simulations on the iLOC attack using real-world traces. Our data show that the iLOC attack can accurately identify monitors while being invisible to ITM systems. Finally, we present a set of guidelines to counteract the iLOC attack.

Index Terms — Internet Threat Monitoring, Invisible Localization Attack, PN-Code, Security, Attack Traffic, Traffic Rate.

1. INTRODUCTION

In current years, we dispread attacks such as worms and distributed denial-of-service (DDoS) attacks have been dangerous threats to the Internet. This section discusses how optimization of recent attacks using IP is achieved the concept Internet Threat Monitoring (ITM) systems have been deployed to detect widespread attacks on the Internet. However, the effectiveness of ITM systems critically depends on the confidentiality of the location of their monitors. If adversaries learn the monitor locations of an ITM system, they can bypass the monitors and focus on the uncovered IP address space without being detected. A system has developed a new class of attacks, the invisible LOCalization (iLOC) attack. The iLOC attack can accurately and invisibly localize monitors of ITM systems. In the iLOC attack, the attacker launches low-rate port-scan traffic, encoded with a selected Pseudo Noise code (PN-code), to targeted networks. While the secret PN-code is invisible to others, the attacker can accurately determine the existence of monitors in the targeted networks based on whether

the PN-code is embedded in the report data queried from the data center of the ITM system.

The ITM builds a better design decouples the processing of IPsec and regular traffic and allows for a balance between both. Its capability to better cope with DoS attacks and demanding applications, especially if QoS support is used.

A system has formally analyzed the impact of various parameters on attack effectiveness. A system has implemented the iLOC attack and conducts the performance evaluation on a real-world ITM system to demonstrate the possibility of such attacks and also conduct extensive simulations on the iLOC attack using real-world traces. The system data shows that the iLOC attack can accurately identify monitors while being invisible to ITM systems.

1.1 INVISIBLE LOCATION ATTACK

The figure 1.1 describes the basic overview of the iLOC attack and the basic idea of the ITM system. In the ITM system, monitors deployed at various networks record their observed port-scan traffic and continuously update their traffic logs to the data center. The data center first summarizes the volume of port-scan traffic toward (and reported by) all monitors and then publishes the report data to the public in a timely fashion. Here the background traffic refers to aggregate traffic collected by the data center but not generated by iLOC attacks.

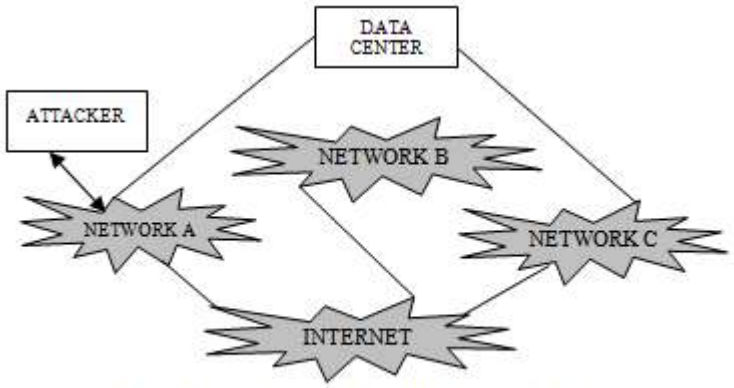


Figure 1.1 Overview of the iLOC attack

Attack traffic generation: In figure 1.2, the attacker first selects a code and encodes the attack traffic by embedding a selected code. The attacker then launches the attack traffic toward a target network (e.g., network A in figure 1.2). A system has denote such an embedded code pattern in the attack traffic as

the attack mark of the iLOC attack and denote the attack traffic encoded by the code as attack mark traffic.

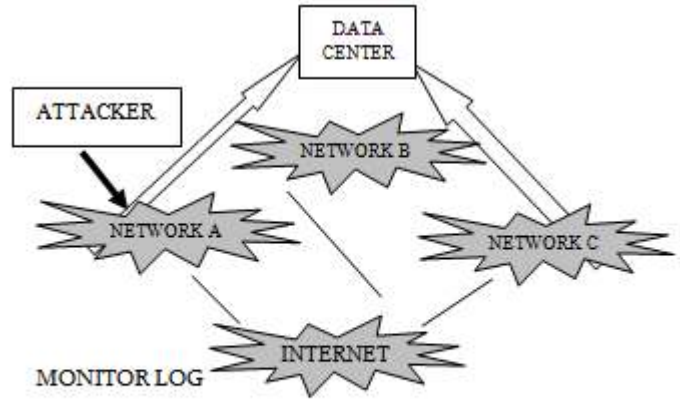


Figure 1.2 Workflow of attack traffic generation

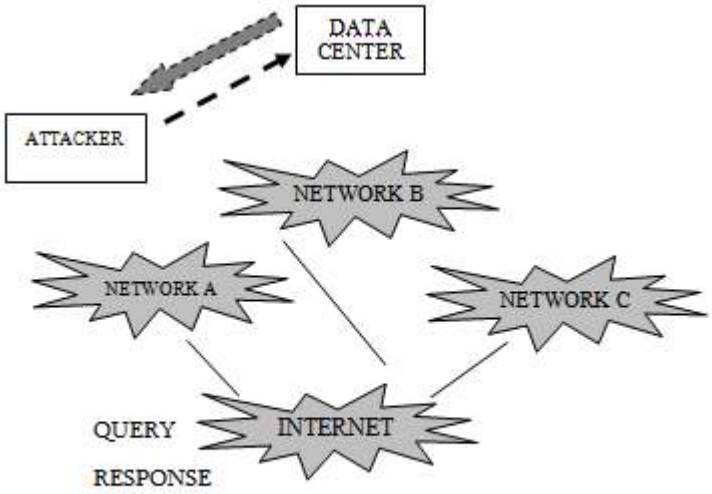


Figure 1.3 Workflow of attack traffic decoding

Attack traffic decoding: In figure 1.3, the attacker first queries the data center for the traffic report data. Such report data consist of both attack traffic and background traffic. Given the report data, the attacker tries to recognize the attack mark (i.e., the code embedded in the iLOC attack traffic) by decoding the

report data. If the attack mark is recognized, the report data must include the attack traffic, which means the target network is deployed with monitors and the monitors are sending traffic reports to the data center of ITM systems.

2. IMPLEMENTATION DETAILS OF Iloc

In this iLOC attack stage, the attacker 1) selects the code, which is a PN-code in the system case, 2) encodes the attack traffic using the selected PN-code, and 3) sends the encoded attack traffic toward the target network. In the third step, the attacker can coordinate a large number of compromised to generate the attack traffic.

2.1 CODE SELECTION

To evade detection, the attack traffic should be similar to the background traffic. From a large set of real-world traffic traces, a system has concluded that the background traffic shows random patterns in both the time and frequency domains. The attack objectives of both accuracy and invisibility and an attacker's desire for parallel attacks require that 1) the encoded attack traffic should blend in with background traffic, i.e., be random in both the time and frequency domains, 2) the code embedded in the attack traffic should be easily recognizable to the attacker alone, and 3) the code should support parallel attacks on the same port. To meet the above requirements, the proposed system chooses the PN-code to encode the attack traffic. The PN-code in the iLOC attack is a sequence of -1 or +1 with the following features.

- The PN-code is random and "balanced." The -1 and +1 are randomly distributed, and the occurrence frequencies of -1 and +1 are nearly equal. This feature contributes to good spectral density properties (i.e., equally spreading the energy over all frequency bands). It makes the attack traffic appear as noise and blend in with background traffic in both the time and frequency domains.
- The PN-code has a high correlation to itself and a low correlation to others (such as random noise), where the correlation is a mathematical utility for finding repeating patterns in a signal. This makes it feasible for the attacker to accurately recognize attack traffic (encoded by the PN-code) from the traffic report data, even under the interference of background traffic.
- The PN-code has a low cross-correlation value among different PN-code instances. The lower this cross-correlation value, the less interference among multiple attack sessions in parallel attack. This makes it feasible for

the attacker to conduct parallel attacks toward multiple target networks on the same port.

2.2 ATTACK TRAFFIC ENCODING

During the attack traffic encoding process, each bit of the selected PN-code is mapped to a unit time period T_s, denoted as mark-bit duration. The entire duration of launched attack traffic is T_sL, where L is the length of the PN-code. After the attacker launches port scans to target networks, they also queries the data center for the traffic report periodically. For brevity, this query interval is set to T_s.

The encoding is conducted based on the following rules – each bit of the PN-code maps to a mark-bit duration T_s; when the PN-code bit is +1, port-scan traffic with a high rate, denoted as mark traffic rate V, is generated in the corresponding mark-bit duration; when the code bit is -1, no port-scan traffic is generated in the corresponding mark-bit duration. Thus, the attacker embeds the attack traffic with a special pattern, i.e., the original PN-code. Recall that after this encoding process, the PN-code pattern embedded in traffic is denoted as the attack mark. Figure 6.4 shows one example of the PN-code and the corresponding attack traffic encoded with the PN-code.

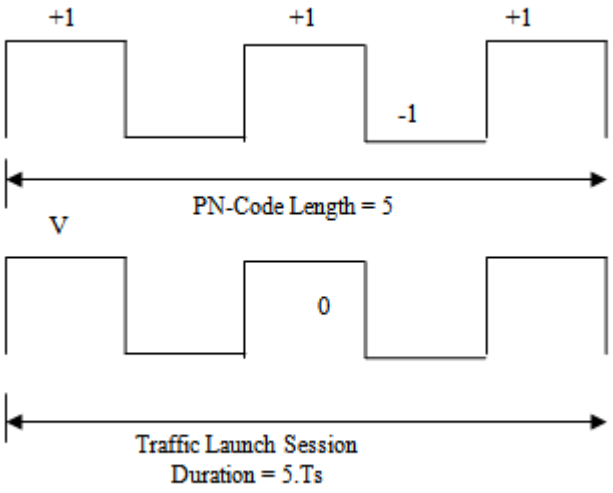


Figure 2.1 PN-code and encoded attack traffic

2.3 ATTACK TRAFFIC DECODNG

In the attack traffic decoding stage, the attacker takes the following two steps,

- The attacker queries the data center for the traffic report data, which consist of both the attack traffic and the background traffic.
- From the report data, the attacker attempts to recognize the embedded attack mark. The existence of the attack mark determines whether the targeted network is deployed with monitors or not. As the query of traffic report data is relatively straightforward, the system only details the second step, i.e., attack mark recognition, as follows.

In the report data queried from the data center, the attack traffic encoded with the attack mark is mixed with the background traffic, which is aggregated by the data center but not generated by iLOC. It is critical for the iLOC attack to accurately recognize the attack mark from the traffic report data. To address this, the system has developed a correlation-based scheme. This scheme is motivated by the fact that the original PN-code (used to encode attack traffic) and its corresponding attack mark (embedded in the traffic report data) are highly correlated: in fact, they are sharing the same pattern. The attack mark in the traffic report data is the embedded form of the original PN-code. The attack mark is similar to its original PN-code, although the background traffic may introduce interference and distortion into the attack mark.

3. DESIGN

In order to design the optimization of recent attack to find out the accuracy in terms of how correctly the attacker is able to recognize the probe mark and identify monitor location, the system has introduced the following two metrics. The first one is the attack success rate PA_D, the probability that an attacker correctly determines that a selected target network is deployed with monitors. From the attacker's perspective, the higher PA_D is better the attack accuracy. The second metrics is the attack false-positive rate PA_F, the probability that the attacker mistakenly determines a target network as one with monitors. From the attacker's perspective, the lower PA_F is, the better the attack accuracy.

3.1 MODIFIED IMPLEMENTATION OF iLOC ATTACK

There are five independent and important components in modified implementation of iLOC attack, as shown in figure 3.1. The modified iLOC is implemented in Microsoft MFC and Matlab on Windows XP OS. The five components are described as follows,

- **Background Traffic Analyzer.** This component receives the data of background port-scan traffic on given ports via the Data Center Querist. With such data, this component obtains the statistic profile of background

traffic, e.g., standard deviation σ_x. The profile is used to determine attack parameters for other components.

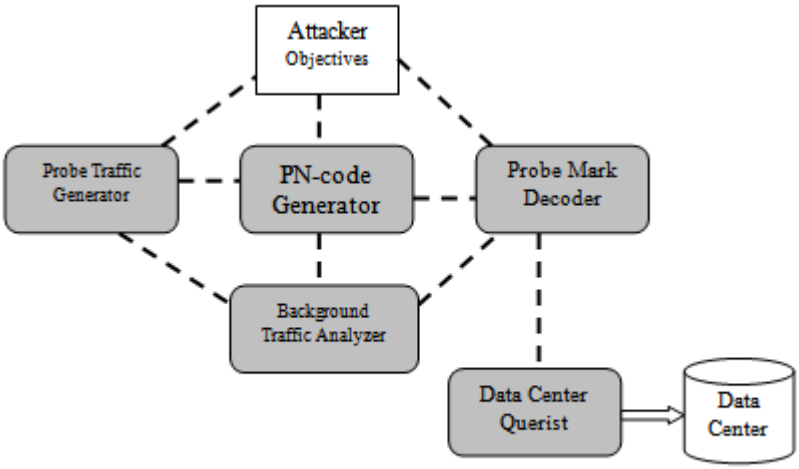


Figure 3.1 Implementation of iLOC Components

- **PN-code Generator.** This component generates and stores a PN-code. The PN-code length is determined according to the attacker's objectives and the background traffic profile in the way. Recall that the system has used the feedback shift register to generate the PN-code. The feedback shift register repeatedly generates a PN-code of length L.
- **Probe Traffic Generator.** This component generates attack traffic based on the PN-code and the statistic profile of background traffic. With the profile of the background traffic, the attack traffic rate is determined based on the method. The PN-code encoded traffic is generated in a way as discussed. The inputs to this component are the IP addresses of the target network, the port number, and the transportation protocol (TCP or UDP).
- **Probe Mark Decoder.** This component obtains the port-scan report data through the Data Center Querist and decides whether the probe mark exists in the way discussed. The PN-code used in the decoding process is the same one used in encoding attack traffic and stored in the PN-code Generator. The decoding threshold is determined by this component based on the attack accuracy requirement and the background.

4. SIMULATIONS AND PERFORMANCE EVALUATION

The evaluation should be carried out over a real ITM system in an ideal situation. Since an extensive experiment on a real ITM system will affect its usability (e.g., generating skewed reports of the actual Internet traffic), in system evaluation, the system has considered both experiments with a real-world ITM system and simulations using offline traffic traces. In order to validate the system iLOC implementation, the system carried out experiments with a real-world threat monitoring system, SANs ISC, shown in figure 4.1.

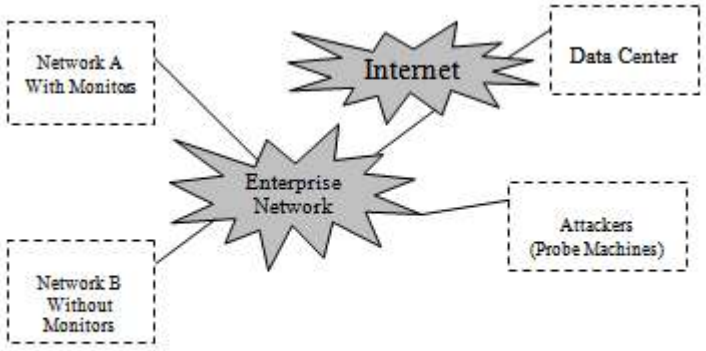


Figure 4.1 Performance Setup

The system has developed to provide with the identities of two networks A and B. There are some monitors in network A, and there is no monitor in network B. The monitors in network A monitor a set of IP addresses and log the port scans. The system has (the attacker) execute the iLOC attack to decide whether monitors exist in network A and B, respectively.

Despite these merits, biometric authentication has some imperfect features. Unlike password, biometric characteristics cannot be easily changed or revoked. Some biometric characteristics (e.g., fingerprint) can be easily obtained without the awareness of the owner. This motivates the three-factor authentication, which incorporates the advantages of the authentication based on password, smart card, and biometrics.

4.1 SIMULATION RESULTS

Optimization are measured based on parameters like attack accuracy, impact of the code length, number of parallel localization attacks and query duration. The average optimization of networks on the various parameters against Attack Success Rate is computed for Attack Traffic Rate.

- The average attack accuracy is to represents the attack success rate in different ports of the whole system in different traffic rate.
- The average impact of the code length is to represents the attack success rate in different length of the whole system in different traffic rate.
- The average number of parallel localization attacks is to represents the attack success rate in different nodes of the whole system in different traffic rate.
- The average query duration is to represents the attack success rate in different length of the whole system in different traffic rate

4.1.1 ATTACK ACCURACY ANALYSIS

Attack Success Rate									
Port No	Traffic Rate = 0.5		% Of savings	Traffic Rate = 1		% Of savings	Traffic Rate = 1.5		% Of savings
	BiLOCA	PiLOCA		BiLOCA	PiLOCA		BiLOCA	PiLOCA	
4321	0.05	0.6	75	0.2	0.9	45	0.35	1	35
135	0.04	0.75	80	0.04	0.95	65	0.05	1	95
25	0.03	0.65	78	0.07	0.95	55	0.08	1	90

Table 4.1 Performance comparison of PiLOCA with BiLOCA for attack accuracy with various attack traffic rate

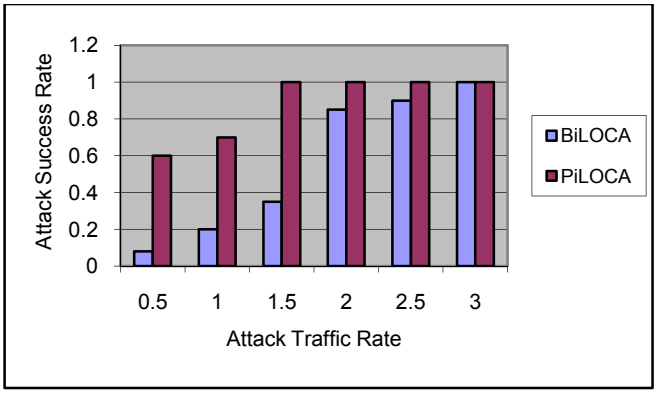


Figure 4.2 Average attack success comparisons with port no 4321

The performance comparison of Proposed iLOC Attack (PiLOCA) with Basic iLOC Attack (BiLOCA) for attack accuracy varies with the attack traffic rate in Table 4.1. Through the implementation of the PiLOCA an increase of attack

accuracy is achieved for various attack success rate with respect to attack traffic rate.

The comparisons with port no 135, which is the average attack success rate for increasing attack traffic rate is given in Table 4.1. The Figure 4.3 shows the comparison with port no 135 while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 58 % when compared with BiLOCA.

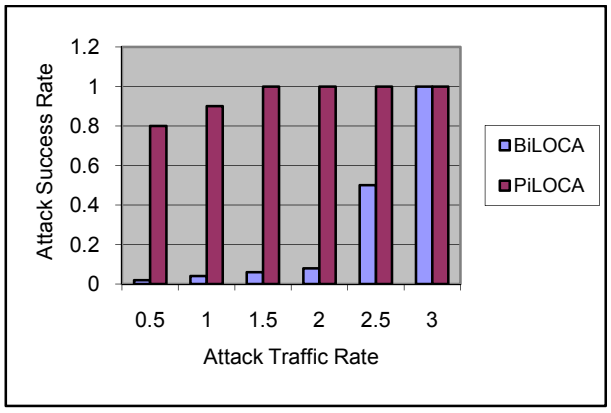
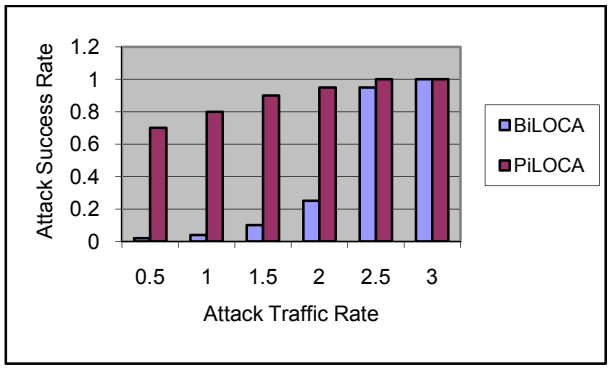


Figure 4.3 Average attack success comparisons with port no 135



4.4 Average attack success comparisons with port no 25

The comparisons with port no 25, which is the average attack success rate for increasing attack traffic rate is given in Table 6.1. The Figure 4.4 shows the comparison with port no 25 while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 75 % when compared with BiLOCA.

4.1.2 IMPACT OF THE CODE LENGTH ANALYSIS

The performance comparison of Proposed iLOC Attack (PiLOCA) with Basic iLOC Attack (BiLOCA) for impact of the code length varies with the attack traffic rate in Table 4.2. Through the implementation of the PiLOCA an increase of impact of the code length is achieved for various attack success rate with respect to attack traffic rate.

Attack Success Rate									
Length	Traffic Rate = 0.5		% Of savings	Traffic Rate = 1		% Of savings	Traffic Rate = 1.5		% Of savings
	BiLOCA	PiLOCA		BiLOCA	PiLOCA		BiLOCA	PiLOCA	
15	0.73	0.78	3.5	0.95	0.98	4	0.97	0.98	2.1
30	0.92	0.98	5.5	0.96	0.99	4	0.98	0.99	2.1
45	0.95	0.99	5.9	0.99	1	1.1	0.99	1	1.1

Table 4.2 Performance comparison of PiLOCA with BiLOCA for impact of the code length with various attack traffic rate

The comparison with impact of the code length 15, which is the average attack success rate for increasing attack traffic rate, is given in Table 6.2. The Figure 4.5 shows the comparison with impact of the code length 15 while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 4 % when compared with BiLOCA.

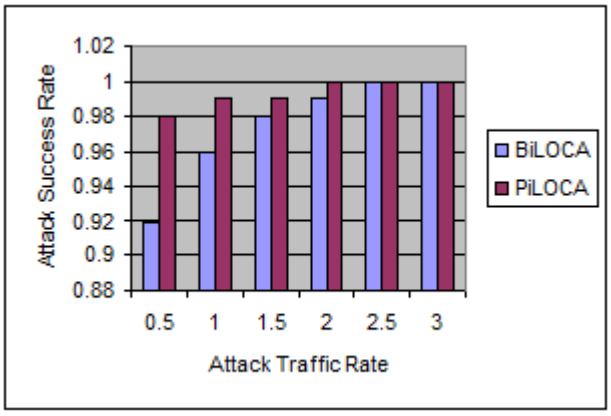


Figure 4.5 Average attack success comparisons with code length 15

The comparison with impact of the code length 30, which is the average attack success rate for increasing attack traffic rate, is given in Table 4.2. The Figure 4.6 shows the comparison with impact of the code length 30 while increasing

attack traffic rate. The attack accuracy for the PiLOCA is increases by 4.5 % when compared with BiLOCA.

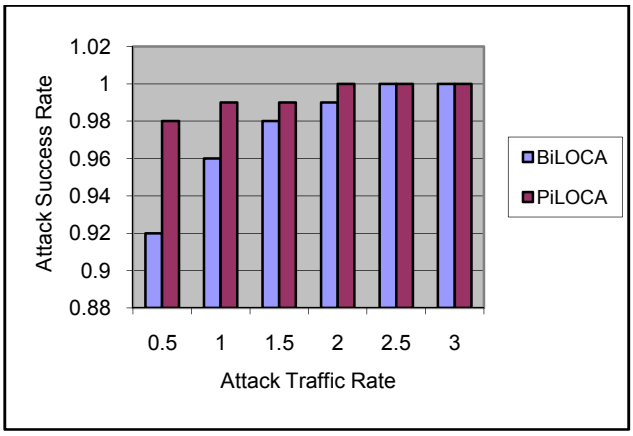


Figure 4.6 Average attack success comparisons with code length 30

The comparison with impact of the code length 45, which is the average attack success rate for increasing attack traffic rate, is given in Table 4.2. The Figure 4.7 shows the comparison with impact of the code length 45 while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 3.5 % when compared with BiLOCA.

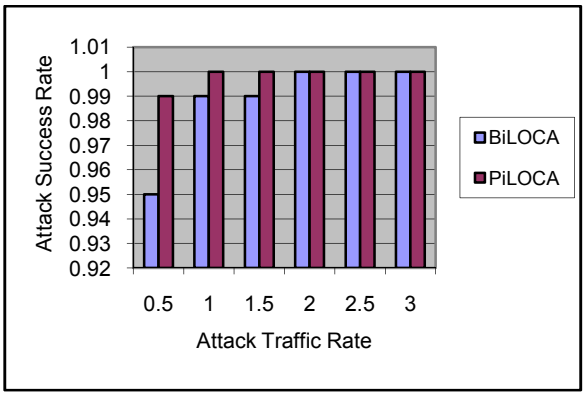


Figure 4.7 Average attack success comparisons with code length 45

4.1.3 NUMBER OF PARALLEL LOCALIZATION ATTACKS ANALYSIS

The performance comparison of Proposed iLOC Attack (PiLOCA) with Basic iLOC Attack (BiLOCA) for number of parallel localization attacks with the

attack traffic rate in Table 4.3. Through the implementation of the PiLOCA an increase of number of parallel localization attacks is achieved for various attack success rate with respect to attack traffic rate.

Attack Success Rate									
Nodes	Traffic Rate = 0.5		% Of savings	Traffic Rate = 1		% Of savings	Traffic Rate = 1.5		% Of savings
	BiLOCA	PiLOCA		BiLOCA	PiLOCA		BiLOCA	PiLOCA	
2	0.92	0.98	5	0.98	0.99	1.5	0.99	1	1.5
4	0.85	0.89	4.5	0.96	0.97	1.5	0.99	1	1.5
8	0.78	0.82	4.5	0.93	0.95	3	0.99	1	1.5

Table 4.3 Performance comparison of PiLOCA with BiLOCA for no. of parallel localization attacks with various attack traffic rate

The comparison with number of parallel localization attacks in 2 nodes, which is the average attack success rate for increasing attack traffic rate, is given in Table 4.3. The Figure 4.8 shows the comparison with number of parallel localization attacks in 2 nodes while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 4.5 % when compared with BiLOCA.

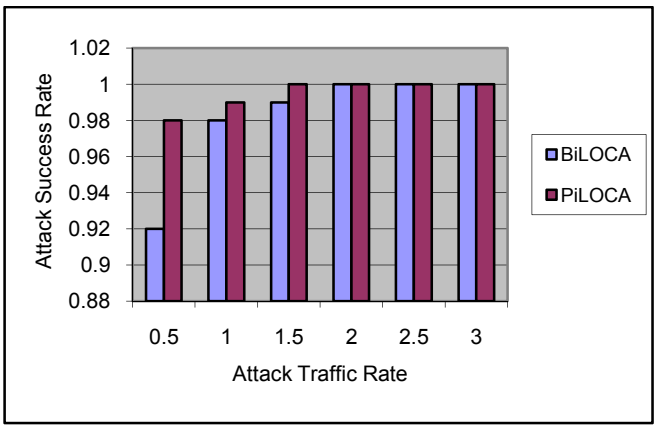


Figure 4.8 Average attack success Vs parallel attacks in 2 Nodes

The comparison with number of parallel localization attacks in 4 nodes, which is the average attack success rate for increasing attack traffic rate, is given in Table 4.3. The Figure 4.9 shows the comparison with number of parallel localization attacks in 4 nodes while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 2 % when compared with BiLOCA.

The comparison with number of parallel localization attacks in 8 nodes, which is the average attack success rate for increasing attack traffic rate, is given in Table 4.3. The Figure 4.10 shows the comparison with number of parallel localization

attacks in 8 nodes while increasing attack traffic rate. The attack accuracy for the PiLOCA is increases by 1.5 % when compared with BiLOCA.

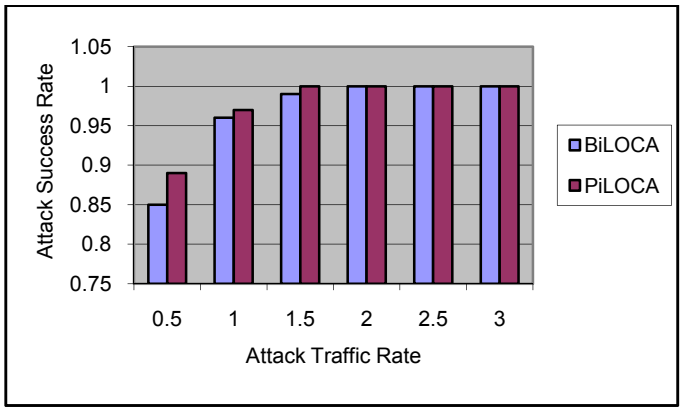


Figure 4.9 Average attack success Vs parallel attacks in 4 Nodes

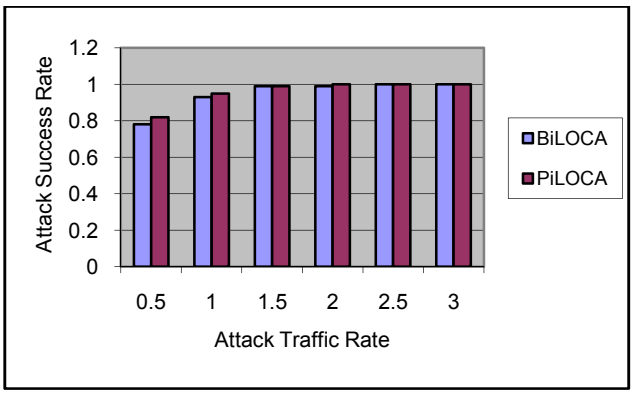


Figure 4.10 Average attack success Vs parallel attacks in 8 Nodes

4.1.4 QUERY DURATION ANALYSIS

The performance comparison of Proposed iLOC Attack (PiLOCA) with Basic iLOC Attack (BiLOCA) for query duration with the attack traffic rate in Table 4.1. Through the implementation of the PiLOCA a decreases of query duration is achieved for various attack success rate with respect to attack traffic rate. The comparison with various lengths, which is the average attack success rate for increasing attack traffic rate. The Figure 4.11 shows the comparison with various lengths while increasing attack traffic rate. The query duration for the PiLOCA is decreases by 5 % when compared with BiLOCA.

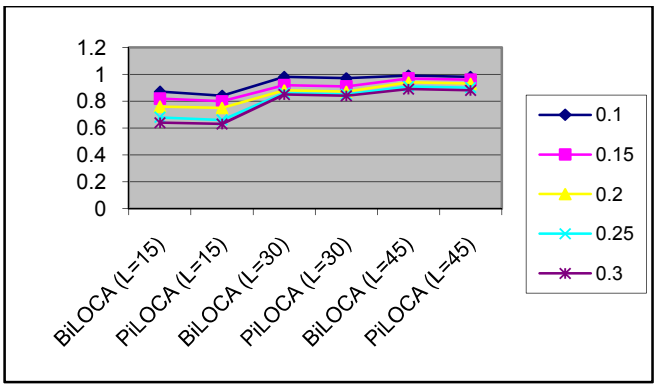


Figure 4.11 Average attack success Vs Query duration

5. CONCLUSION

The establishing an optimization of recent attacks using Internet Protocol. A PiLOCA is developed to find the attack success rate during the various data transfer. The PiLOCA developed here considers the attack accuracy, impact of the code length, number of parallel localization attacks and query duration for stable distance selection criteria. The PiLOCA shows increases in the attack success rate compared to the BiLOCA. The PiLOCA has increased 75% of attack success rate in attack accuracy, increased 3.5 % of attack success rate in impact of the code length, increased 4.5 % of attack success rate in number of parallel localization and has decreased up to 5% of success rate in query duration.

6. REFERENCES

1. Fariba Haddadi, Sara khanchi, Mehran Shetabi, and Vali Derhami (2010), 'Intrusion Detection and Attack Classification Using Feed-Forward Neural Network', Proceedings of 2nd International Conference on Computer and Network Technology, pp. 262-266.
2. Ferrante A, Piuri V, and Castanier F (2005), 'A QoS enabled packet scheduling algorithm for IPSec multi accelerator based systems', Proceedings of the 2nd International Conference on Computing frontiers, pp. 221-229.
3. Fineberg V (2002), 'A practical architecture for implementing end-to-end QoS in an IP network', IEEE Journal on Communication Magazine, Vol. 40, No. 1, pp. 122-130.
4. Francis P, Handley M, Karp R, and Shenker S (2002), 'A scalable content-addressable network', IEEE Journal on Information Computing, pp. 1190-1199.

5. Gao L (2001), 'On inferring autonomous system relationships in the Internet', IEEE Journal on Transactions of Networking, Vol. 9, No. 6, pp. 733-745.
6. Ghandeharizadeh S, Song S, and Krishnamachari B (2004), 'Placement of continuous media in wireless peer-to-peer networks', Proceedings of International Conference on Transactions Multimedia, Vol. 6, Issue 2, pp. 335-342.
7. Giaffreda (2001), 'Name resolving and routing in mobile networks', Proceedings of 2nd International Conference on 3G Mobile Communication Technologies, pp.191-195.
8. Govindan R, Estrin D, and Silva F (2003), 'Directed Diffusion for Wireless Sensor Networking', IEEE Journal on Transactions of Networking, Vol. 11, No. 1, pp. 2-16.
9. Haas, and Pearlman (2001), 'The performance of query control schemes for the zone routing protocol', ACM Journal on Transactions of Networking, Vol. 9, No. 4, pp. 427-438.
10. Haim Zlatokrilov, and Hanoch Levy (2008), 'Area avoidance routing in Distance-Vector networks', IEEE Journal on Communication Society 2008, pp. 1148-1156.
11. Heinzelman W, Kulik J, and Balakrishnan H (1999), 'Adaptive protocols for Information Dissemination in Wireless Sensor Networks', Proceedings of International Conference on Mobile Communication, pp. 174-185.
12. Huayang Cao, Miao Wang, Xiaoqiang Wang, and Peidong Zhu (2009), 'A Packet-based Anomaly Detection Model for Inter-domain Routing', Proceedings of International Conference on Networking, Architecture, and Storage, pp.192-195.
13. HuBaux, Buttyan, and Capkun (2001), 'The quest for security in mobile ad hoc networks', Proceedings of International Conference on Mobile host Communication, pp. 146-155.
14. Jaideep Chandrashekar, Zhenhai Duan, and Xin Yuan (2006), 'Controlling Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates', IEEE Journal on Communications Society, pp.341-352.
15. Jayanth, and Bharghavan (1998), 'Performance of transport protocols over a multicasting based architecture for Internet host mobility', IEEE Journal on Communication Society 1998, pp. 1817-1823.
16. Jingyuan Li, Liusheng Huang, Weijia Jia, Mingjun Xiao, and Peng Du (2006), 'Systems on the basis of WiMAX and Wi-Fi', IEEE Journal on Communication Society, pp. 819-824.

17. Jirapummin C, Wattanapongsakorn N, and Kanthamanon P (2002), 'Hybrid neural networks for intrusion detection system', Proceedings of International Conference on Circuits, Computers and Communications, pp. 928-931.
18. Johnson D, Maltz A, and Broch J (2001), 'DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad hoc Networks', IEEE Journal on Ad hoc Networking, pp. 139-152.

AUTHORS' PROFILE:

A.Rengarajan received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2000 and the Post Graduate degree in Computer Science and Engineering from Sathyabama University, Chennai in 2007. He is currently doing her research in Faculty of Computer Science Engineering at Bharath University, Chennai-73. He has more than 10 publications in National Conferences and international journal proceedings. He has more than 8 years of teaching experience. His areas of interest include Data Mining, Data Structures, DBMS, Distributed systems and Operating systems.

C.Jayakumar has more than 14 years of teaching and research experience. He did his Postgraduate in ME in Computer Science and Engineering at College of engineering, Guindy, and Ph.D in Computer Science and Engineering at Anna University, Chennai. He has published more than 35 research papers in High Impact factor International Journal, National and International conferences and visited many countries like USA and Singapore. He has guiding a number of research scholars in the area Adhoc Network, Security in Sensor Networks, Mobile Database and Data Mining under Anna University Chennai, Anna University of Technology , Sathayabama University and Bharathiyar University. He conducted Various National Conferences, Staff Development Program, Workshop, Seminar in associated with Industries like Infosys and TCS. He has Received Rs 22 Lakhs Grant from AICTE for RPS Project and Staff Development Program. He Chaired various International and National Conferences. He was Advisor and Technical Committee Member for many International and National Conferences. Currently he working as Professor in the Department of Computer Science and Engineering, RMK Engineering College

Sugumar.R received the Undergraduate Degree in Computer Science and Engineering from Madras University, in 2003 and the Post Graduate degree in Computer Science and Engineering from Dr.M.G.R. Educational and Research Intituite, Chennai in 2007. He is currently doing her research in Faculty of Computer Science Engineering at Bharath University; Chennai-73.He has more than 5 publications in National Conferences and international journal proceedings. He has more than 8 years of teaching experience. His areas of interest includes Data Mining, Data Structures, DBMS, Distributed systems and OS.