THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Efficient Game-Theoretic Approach for Malware Detection in Delay-Tolerant Networks

Jayalekshmi S.
M.E. Computer Science and Engineering, Nehru Institute of Technology, Coimbatore, India
M. Jeba Kumari
Associate Professor, Department of CSE, Nehru Institute of Technology, Coimbatore, India

Abstract:
Delay Tolerant Networking (DTN) is introduced as an approach in network architecture that is used to address the technical problems in non-homogeneous networks that may reduce continuous network connectivity. Proximity malware is a malware which enters into Networks via Bluetooth, WI-Fi etc. and exploits the opportunistic contacts for propagation. The behavioral characterization of malware is an alternative approach to pattern matching for detecting proximity malware. Since there is a risk associated with a decision in behavioral malware characterization, an extension named Look Ahead is introduced in this work. Furthermore, two extensions are developed such as Adaptive Look ahead and Dogmatic filtering to remove the challenge of evil nodes sharing false evidences. In the proposed research, a Game Theoretic approach for malware detection is introduced. The game theory provides a powerful mathematical tool having huge number of players. The proposed system achieves a high detection rate than previous approaches.

Keywords*: Adaptive Look Ahead, Behavioral malware Detection, Delay Tolerant Networks, Dogmatic Filtering, Game theory, proximity malware*

1. Introduction

The popular mobile consumer electronic products such as Laptops, PDAs, and smart phones make the Delay Tolerant Networks an alternative to the traditional infrastructure model. Proximity malware is a class of malware that specially targets the Delay Tolerant Networks. Symbian based Cabir Worm is one example of this malware which enters through the Bluetooth Link between two devices. IOS based Ikee Worm is another example, which propagates through wireless connections. Proximity malware gives more security challenges to DTN since cellular carrier which centrally monitors networks for irregularities in infrastructure model is not present in DTN model. Proximity malware can take advantage of the opportunistic contacts of DTNs for propagation. One way of defending against malware is to detect it based on behavioral characterization which is introduced in this paper. The behavioral characterization, with respect to system calls and program flow is projected as an efficacious alternative to pattern matching for detecting malware. In this model, malware-infected node's behavior is observed by others during their multiple opportunistic encounters. Individual observations may be found to be imperfect, but anomalous behaviors' of infected nodes are identifiable in the long-run. Basically, a Naïve Bayesian Model is developed. Then Look Ahead is added for addressing the challenges such as 'Insufficient Evidence and Evidence Collection Risk'. Moreover two extensions, namely Adaptive Look Ahead and Dogmatic Filtering are developed for addressing the challenges of Liars and Defectors. In order to enhance the detection rate and performance, a Game Theoretic approach is introduced. It acts as a powerful mathematical tool having many players capable of taking security decisions without centralized administration. The main objective of this research is to design an effective optimal detector algorithm taking into account attacker strategies and actions for detecting malware in the delay-tolerant networks.

2. Related Works

For countering malware attacks a number of techniques have been reported in recent times. Distributed malware detection based on binary file features in cloud computing environment by Xiaoguang Han; Jigang Sun; Wu Qu; Xuanxia Yao (2014): Machine learning techniques play an important role in malware detection. In this paper a binary file to image projection algorithm based on feature extraction is introduced to face the challenge of growing array of countermeasures. Also a distributed (key, value) abstraction in a cloud computing environment is introduced to face the challenge of time investment per binary file. The proposed method could be useful and efficient for dynamic analysis complementation.

Scalable approach for malware detection through bounded feature space behavior modeling by Chandramohan, M.; Hee Beng Kuan Tan; Briand, L.C.; Lwin Khin Shar; Padmanabhuni, B.M. (2013): The practical difficulty in detecting the malware using behavior-based malware detection techniques is addressed in this paper. A Bounded Feature Space Behaviour modeling (BOFM) for scalable malware detection is proposed. It can model the interactions among software and security critical OS resources. In this technique, the computation time and usage of memory are lower than other techniques .Also high detection accuracy is another advantage.

On behavior-based detection of malware on Android platform by Yu Wei; Hanlin Zhang Linqiang Ge; Hardy, R. (2013): The increased growth of mobile devices makes possible more malware attacks on it. For addressing this issue, a behavior based detection approach is used for malware detection. In order to achieve this, here the system calls to attain the run-time behavior of software and adopt machine learning approaches such as Support Vector Machine (SVM) are presented. Also Naïve Bayesian learning techniques to study the dynamic behavior of software execution are proposed. This technique is effective in terms of algorithm learning.

Behavior-Based Malware Analysis and Detection by Liu Wu; Ren Ping; Liu Ke; Duan Hai-xin (2011): The main malwares which threaten the internet are virus, worms, Trojans etc. The content signatures vary due to malware and its variants. In this paper, investigations are made on the extraction of malware behavior and the formal Malware Behavior Feature (MBF) extraction method is introduced. Thus a malicious behavior-based malware detection algorithm is proposed. The implementation of this technique shows that it can detect newly formed unknown malwares.

3. Existing System

In the existing system, a simple, yet effective solution called look ahead, which naturally reflects individual node's intrinsic risk inclinations against malware infection is presented. Subsequently the naive Bayesian model, which has been applied in filtering email spams, detecting botnets, and designing Intrusion Detection Systems and address two DTN specific, malware-related, problems namely-insufficient evidence versus evidence collection risk is introduced. In DTNs, evidence is collected only when nodes are in contact. But contact with the malware-infected nodes carries the risk of being infected. Thus, nodes must make decisions based on potentially insufficient evidence. The behavioural malware characterization represents the malware detection process as a distributed decision problem. When analyzing the risk associated with the decision, a simple, yet effective strategy, look ahead, which naturally reflects individual node's intrinsic risk inclinations against malware infection, is designed. Look ahead extends the naive Bayesian model and addresses the DTN specific, malware-related, 'insufficient evidence versus evidence collection risk' problem. Then two alternative techniques, dogmatic filtering and adaptive look ahead, that naturally consolidate evidence provided by others, while having the negative effect of false evidence. The disadvantages of existing system are less detection accuracy and efficiency.

4. Proposed System

In the proposed method, the mean field game theory is used for malware detection in delay-tolerant networks. The mean field game theory provides a powerful mathematical tool for problems with a large number of players which proves to be of tremendous help to economists, socialists and engineers. A dynamic mean field game theoretic approach is proposed to enable an individual node in DTN to make strategic security defense decisions without centralized administration. The proposed scheme considers not only the security requirement of delay-tolerant networks but also the system resources. In this scheme each node needs to know only its own state information and the aggregate effect of the other nodes in the delay-tolerant networks. The advantages of proposed system are high detection accuracy and more efficiency.

4.1. Proposed Algorithm

Initialize N number of nodes in the network , $N = n_1, n_2, \dots n_i$

Probability of the network routing or set of detectors being in a specific state is given by the vector $X = [x_1, \dots, x_{R_{max}}]$ where $0 \le x_i \le 1$ and $\sum_{i=1}^{R_{max}} x_i = 1$

Transition probabilities are described by transition matrix M

Every player is associated with a set of costs

The cost of the IDS is defined as, $-c(R_i, D_i, A_j)$

The cost of the attacker is defined as $c(R_i, D_i, A_j)$ Where $R_i \in R, D_i \in D, A_j \in A$

The cost function of the attacker is denoted as,

$$c(s_i, A_i, D_j) = \begin{cases} 1 & if\ D_j \in p(s_i, A_i) \\ -1 & otherwise \end{cases}$$ // Where $p(s_i, A_i)$ denote the path of the packets of attack

Markov decision processes' value,

$$V(s) = \min_{\Pi^A} \max_{o \in D} \sum_{a \in A} Q(s, a, o)\Pi^A$$

$$Q(s, a, o) = R(s, a, o) + \gamma \sum_{s' \in S} T(s, s')V(s')$$ // Where T=state transition matrix, $Q(s, a, o)$ is the expected reward for taking action

The optimal strategy of the player, $\Pi^A = arg\ \min_{\Pi^A} \max_{o \in D} \sum_{a \in A} Q(s, a, o)\Pi^A$ // Π^A = attacker strategy matrix, Π_{ij}^A denotes the probability of choosing attack pattern, Π_{ij}^D denotes the probability of choosing detection pattern.

Figure 1

5. Overall Architecture

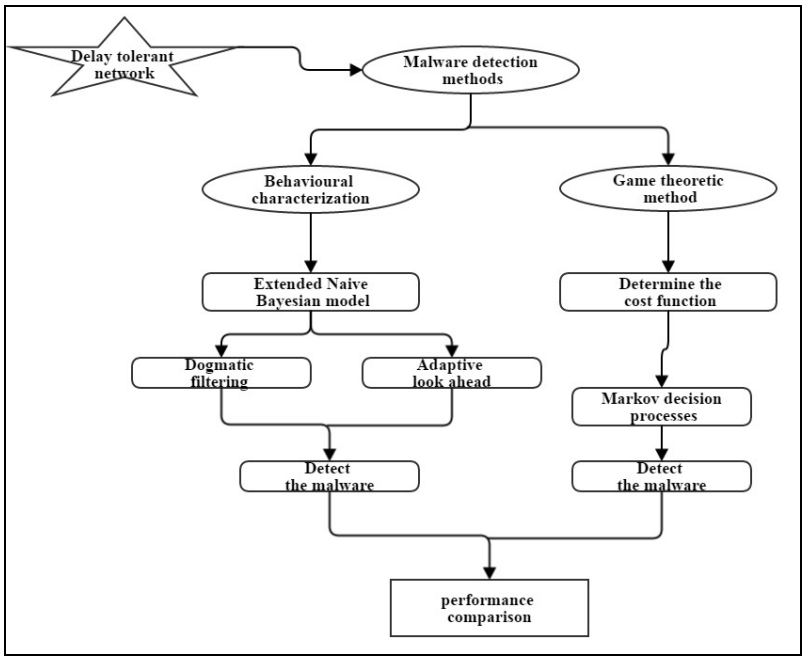

Figure 2

6. Conclusion

Behavioural based malware characterization is an effective alternative to pattern matching in detecting malware, particularly when dealing with polymorphic malware. Naive Bayesian model has been successfully applied in non-delay tolerant networking settings, such as filtering email spams and detecting botnets. A general behavioural characterization of DTN-based proximity malware is proposed in this paper. The look ahead is presented along with dogmatic filtering and adaptive look ahead, to address the unique challenges of extending Bayesian filtering to DTNs namely 'Insufficient evidence versus evidence collection risk' and 'Filtering false evidence sequentially and distributedly. A novel mean field game theoretic approach to model the interactions among a malicious node and a large number of legitimate nodes is added. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. In this method there is high detection rate with less energy consumption.

7. References

1. Xiaoguang Han ; Jigang Sun ; Wu Qu ; Xuanxia Yao (2014). Distributed malware detection based on binary file features in cloud computing environment.
2. Chandramohan, M. ; Hee Beng Kuan Tan ; Briand, L.C. ; Lwin Khin Shar ; Padmanabhuni, B.M.(2013).Scalable approach for malware detection through bounded feature space behaviour modelling
3. Yu Wei ; Hanlin Zhang ; Linqiang Ge ; Hardy, R. (2013). On behaviour-based detection of malware on Android platform
4. Liu Wu ; Ren Ping; Liu Ke; Duan Hai-xin(2011). Behaviour-Based Malware Analysis and Detection
5. C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang,(2009) "Effective and Efficient Malware Detection at the End Host," Proc. 18th Conf. USENIX Security Symp.
6. U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda,(2009) "Scalable, Behaviour-Based Malware Clustering," Proc. 16th Ann. Network and Distributed System Security Symp. (NDSS).
7. F. Li, Y. Yang, and J. Wu, "CPMC: (2010).An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM.
8. R. Villamarı´n-Salomo´n and J. Brustoloni,(2013) "Bayesian Bot Detection Based on DNS Traffic Similarity," Proc. ACMymp. Applied Computing (SAC).
9. Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng,(2011) "An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices," Proc. IEEE Eighth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON).