Address the challenge of "malicious nodes sharing false evidence." The proposed system achieves a high detection rate than previous approaches.

Index Terms—Delay Tolerant Networks, Proximity malware, Game theory, Homomorphic signature scheme.

I. INTRODUCTION

The popularity of mobile consumer electronics, like laptop computers, PDAs, and more recently and prominently, smart phones, revives the delay-tolerant network (DTN) model as an alternative to the traditional infrastructure model. The widespread adoption of these devices, coupled with strong economic incentives, induces a class of malware that specifically targets DTNs. We call this class of malware proximity malware. An early example of proximity malware is the Symbian based Cabir worm, which propagated as a Symbian Software Installation Script (.sis) package through the Bluetooth link between two spatially proximate devices [1]. A later example is the iOS-based Ikee worm, which exploited the default SSH password on jail broken [2] iPhones to propagate through IP-based Wi-Fi connections [3].

Proximity malware based on the DTN model brings unique security challenges that are not present in the infrastructure model. In the infrastructure model, the cellular carrier centrally monitors networks for abnormalities; moreover, the resource scarcity of individual nodes limits the rate of malware propagation. For example, the installation package in Cabir and the SSH session in Ikee which were used for malware propagation, cannot be detected by the cellular carrier. However, such central monitoring and resource limits are absent in the DTN model. Proximity malware exploits the opportunistic contacts and distributed nature of DTNs for propagation. It a malware which enters into Networks via Bluetooth, Wi-Fi etc. and exploits the opportunistic contacts for propagation.

One way of defending against malware is to detect it based on behavioral characterization [4] 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.

II. 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. 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.

III. 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 naïve 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 behavioral 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 naïve 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.

IV. PROPOSED SYSTEM:

In this paper we propose a different solution to the problem of detecting pollution attacks. To detect malware within the network, we design a new homomorphic signature allows nodes to sign any linear combination of the incoming packets without contacting the signing authority. It also provides authentication in addition to detecting pollution. To address the problem created by malware from external network, we propose Game theoretic approach[7] which is a powerful mathematical tool. 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 advantages of proposed system are high detection accuracy and more efficiency.

A. Homomorphic Signature Scheme:

Homomorphic signature scheme is one of the symmetric encryption scheme wherein the sender and the receiver agree on the key they will use before establishing any secure communication session.[5] Therefore, it is not possible for two persons who never met before to use such schemes directly. This also implies that in order to communicate with different persons, we must have a different key for each person.

One of the most interesting applications of homomorphic encryption is its use in protection of mobile agents.[6] Since all conventional computer architectures are based on binary strings and only require multiplication and addition, such homomorphic cryptosystems would offer the possibility to encrypt a whole program so that it is still executable. Hence, it could be used to protect mobile agents against malicious hosts by encrypting them. The protection of mobile agents by homomorphic encryption can be used in two ways: (i) computing with encrypted functions and (ii) computing with encrypted data. Computation with encrypted functions is a special case of protection of mobile agents. In such scenarios, a secret function is publicly evaluated in such a way that the function remains secret. Using homomorphic cryptosystems the encrypted function can be evaluated which guarantees its privacy. Homomorphic schemes also work on encrypted data to compute publicly while maintaining the privacy of the secret data. This can be done encrypting the data in advance and then exploiting the homomorphic property to compute with encrypted data.

![fig.1 Behavioral characterization in malware detection](image-url)
fig 2. Homomorphic signature scheme for malware detection within a network.

B. Game Theory:

Game theory is the formal study of conflict and cooperation. Game theoretic concepts apply whenever the actions of several agents are interdependent. These agents may be individuals, groups, firms, or any combination of these. The concepts of game theory provide a language to formulate, structure, analyze, and understand strategic scenarios.

The mean field game theory is used for malware detection in delay-tolerant networks.\[8\][9][10] 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 defence decisions without centralized administration. The proposed scheme considers not only the security requirements 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.

fig 3. Proposed Algorithm

The mathematical field of game theory provides an extensive set of tools to model real-life network security problems. In particular, attackers attempting to gain unauthorized access to a target system residing in the network or compromise its accessibility through distributed denial of service (DDoS) attacks must be – in the worst case – expected to have complete knowledge of the internal configuration of the network such as routing states or detector locations. Thus, attackers need to be viewed as rational and intelligent players who respond to the actions taken by the IDS by choosing different targets or routes to inject the malware. Due to this adaptive behavior of the opponent, in our view, the approaches mentioned in the previous subsection are not sufficient. More precisely, while the algorithms proposed in the literature will possibly yield large sampling rates over all packets traversing the network, this may not be the case for the sampling rate of infectious packets if the attacker’s behavior is not taken into account. Motivated by the shortcomings of the approaches described above, we model Game theory approach.

➢ ANONYMITY AND PRIVACY

Game theory can help users to decide whether they want to participate in privacy-preserving mechanisms, how much they would be able to contribute and how much privacy they would be able to achieve. We analyze the non-cooperative behavior of mobile nodes by using a game-theoretic model, where each player aims at maximizing its location privacy at a minimum cost where mobile nodes collectively change their pseudonyms in regions called mix zones.

fig 4

Description of the threshold equilibrium in the 2-player incomplete information game. Threshold $\theta_i$ determines the best response of player $i$, $n$ is the number of nodes in the mix zone.

➢ TRUST VS PRIVACY

Network nodes need to disclose some private information, in order to establish trust. This causes a tension between security and trust in Delay tolerant networks. [11][12] Using a game-theoretic approach, we study this tradeoff. They model the strategies of rational users that try to establish data-centric trust in the presence of rational adversaries. The two macro players are A (attacker) and D (defender) with two possible actions: S (send attributes to the information verifier V) and W (wait until the next stage).

When sending, each macroplayer increases the level of trust in its information but the opponent can surpass it in the next stage, thus requiring the first macroplayer to disclose even more attributes in the subsequent stage. The winner has to provide a trust level at least equal to a defined threshold, $\theta$. Let $c$ be the privacy loss required to reach $\theta$. Hence, each macroplayer is required to invest at least an amount $c$ of privacy to win the game. $v_A$ represents how much the attacker benefits from a successful attack, whereas $v_D$ represents the
cost that the defender avoids by preventing the attack.

We first prove that the strategy \((W, WW)\) is a Perfect Bayesian Equilibrium (PBE) of the game.\cite{13}\cite{14} This means that D’s best strategy is to play always W and A’s best-response strategy is to play W regardless of whether D plays W or S. In practice, both macro players wait until the last stage where they rely on their respective probabilities of access to win. This means that the information verifier can decide on the information only at the deadline, which is not desirable. Accordingly, we prove that incentives can enable trust establishment and reduce the amount of disclosed privacy. We analyze the game with incentives and show that the resulting equilibrium is not constrained to waiting. We also analyze show that no misbehaving nodes will be revoked by a voting mechanism unless there are enough incentives for revocation.

E. Network Formation

- The simulation is done in ns2. In the simulation model, there are 50 sensor nodes deployed in a 800x600 m2 field.
- All the nodes are set as static nodes.
- The type of the wireless propagation model is Two Ray Ground. Routing protocol which is used in this simulation is AODV.

V. SYSTEM ARCHITECTURE:

D. Analysis

We will evaluate
- Packet delivery ratio
- Throughput.
- Residual energy.

Several goals are established for the security component of the DTN architecture:

1) Promptly prevent unauthorized applications from having their data carried through the DTN
2) Prevent unauthorized applications from asserting control
over the DTN infrastructure
3) Prevent otherwise authorized applications from sending bundles at a rate or class of service for which they lack permission
4) Promptly discard bundles that are damaged or improperly modified in transit
5) Promptly detect and de-authorize compromised entities.

Most network security methods attempt to mutually authenticate user identities and the integrity of messages but do not attempt to authenticate routers that forward information. In DTNs, forwarding nodes (routers and gateways) are also authenticated, and sender information is authenticated by forwarding nodes, so that network resources can be conserved by preventing the carriage of prohibited traffic at the earliest opportunity.

VI. 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 distributively. 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.

VII. REFERENCES

[7] Xiaoguang Han ; Jigang Sun ; Wu Qu ; Xuanxia Yao (2014). Distributed malware detection based on binary file features in cloud computing environment.
[10]Liu Wu ; Ren Ping; Liu Ke; Duan Hai-xin(2011). Behaviour-Based Malware Analysis and Detection