ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Hybrid Scheme for Malware Detection in Delay Tolerant Networks

Vineetha.S*, Shiva Ranjani.P

*M.Phil Scholar, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, India

Asst. Professor, Department of Computer Applications, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, India

Abstracts

Delay tolerant network (DTN) utilize the mobility of node and opportunistic contact among nodes for data communication. Due to limitation in resources such as buffer space and contact opportunity, DTNs are vulnerable to malware based attack. So the proposal introduces a novel malware detection technique in DTN. The proposed system deals with the several evidence matching and collection problems. The system also identifies the misbehaving nodes by collecting and validating their evidence using ECDSA. The signature and Behavioral analysis of every node along with the evidence collection helps to track the accurate malware in DTN. The proposed system uses a hybrid collaborative malware detection technique to improve the detection accuracy.

Keywords: mobility,malware,evidence,signature,collaborative

Introduction

Delay tolerent network

D***elay*** T***olerant*** N***etworking*** is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. DTN works using different kind of approach than TCP/IP for packet delivery that is more resilient to disruption than TCP/IP. The basic idea behind DTN network is that endpoints aren't always continuously connected. In order to facilitate data transfer, DTN uses a store-and-forward approach across routers that are more disruption-tolerant than TCP/IP. However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity.

Store and forward message switching

DTNs overcome the problems associated with intermittent connectivity, long or Variable delay, asymmetric data rates, and high error rates by using store-and forward Message switching. The storage places (such as hard disk) can hold messages indefinitely. They are called *persistent storage*, as opposed to very short-term storage provided by memory chips and buffers. Internet routers use memory chips and buffers to store (queue) incoming packets for a few milliseconds while they are waiting for their next-hop routing-table lookup and an available outgoing router port.

Intermittent connectivity

An intermittently connected network contains links that become available and unavailable during normal operation. This behavior is caused by mobility of nodes, lack of line-of-sight, physical disconnection, node failure, and transmission power among other factors. Link availability may be scheduled, probabilistic, or random based on the cause of disconnection.

Bundle protocol

The DTN architecture implements store-and-forward message switching by overlaying a new transmission protocol—called the *bundle protocol*—on top of lower-lower protocols, such as the Internet protocols.

DTN security requirement

Authentication

As in conventional systems, authentication techniques verify the identity of the DTN nodes in communication and distinguish legitimate DTN users from unauthorized users. In DTNs,it is essential for every intermediate DTN node to have the capability to verify that the data was really sent by an authorized node, at a legitimate rate or class of service for which they are granted. Such an authentication requirement can be provided either on a hop-by-hop or end-to-end basis, depending on different security design goals.

Confidentiality

The confidentiality objective can be achieved using the end-to-end encryption, which requires the presence of mutual authentication and key agreement between the source and the destination.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Integrity
Integrity requirement should ensure that the transmitted messages can not be altered during the propagation processThe network should not reveal the location of the user, nor the party with which she communicates.

DTN security characteristics
Lack of End-to-end Connectivity
As a major characteristic of DTNs, lack of end-to-end connectivity not only brings challenge to routing but also makes the existing security solutions, which have been well studied in conventional networks, not applicable in DTNs.
Fragmentation
In DTNs, due to high mobility, each network link becomes available only for a short period of time. Therefore, when a message is large, it may not be possible to send the entire message at once. One possible solution is to split the message into smaller pieces and let each become its own bundle, or "fragment bundle", and send some pieces of a large message through the current link and rest of the message through another link later to make the best use of limited resources.

Related and existing work

- There are several common malware detection method currently in practice is pattern matching, which is a supervised data matching technique.
- The existing pattern matching suffers from the following drawbacks
    - Processing overhead the lack of generality,
    - High false positive rate in one round of analysis make it unsuitable for DTN applications in real-time.
- Some work used patching or self-healing themes.
- Late random waypoint method has been applied, recent findings on these techniques show that these models may not be realistic.
- Some techniques designed on the observation that trust evaluations can link past experiences with future predictions.
- Some online provision framework designed on the observation that trust evaluations can link past experiences with future predictions.

Problem definition

Although many schemes have been proposed to defend against malware attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. Thus, it is still an open problem is to address inject attacks in DTNs.

1. Most existing is not a DTN specific,
2. Several existing failed to identify the malware exactly.
3. Suffered from several trust management problems
4. Insufficient evidence versus evidence collection risk and
5. Sequential and distributed online evidence filtering.

Proposed system

- Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware.
- The proposed system applies behavioral characterization for malware detection.
- the proposed system overcomes the insufficient evidence risk and evidence collection risk.
- The proposed system also identifies the fake evidences by applying effective signature schemes.
- The proposed system deal the following security issues DTN
    - injecting
    - Proximity malware
    - Spoofing based attacks
- In existing the Naive Bayesian model has been successfully applied in non-DTN settings, such as filtering email spams and detecting botnets.
- The proposed system implements a general behavioral characterization of DTN-based proximity malware. This presents enhanced look ahead method which is deep evidence inspection, along with dogmatic filtering and adaptive look ahead, to address two unique challenging in extending Bayesian filtering to DTNs:
- "insufficient evidence versus evidence collection risk"
- "Filtering false evidence sequentially and distributedly."

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Research methodologies

The proposed system introduces a new technique which is named as HMD (**Hybrid Malware Detection)** which combines the successful combination of **signature**, **behavior** and **code sequence** based techniques**.** The decentralized approach provides effective sign matching and neighborhood verification process in the network while data transmission.

The proposed system introduces an encounter-based evidence distributed algorithm to disseminate the malware signatures. It only relies on local information and opportunistic contacts.

a. Behavior -based Detection

Behavior based detection differs from the surface scanning method in that it identifies the action performed malware rather than the binary pattern. The programs with dissimilar syntax's but having same behavior are collected, thus this single behavior signature can identify various samples of malware.

The behavior detector basically consists of following components which are as follows:

• **Data Collection:** This component collects the dynamic / static information's are captured.

• **Interpretation:** This component converts the raw information collected by data collection module into intermediate representations.

• **Matching Algorithm:** It is used to compare the representation with the behavior signature.

a. Signature Based detection:

A malware signature consists of the summarized malicious patterns in the malware, which can be included in an alert or a patch. If a node receives the signature before it is infected by a proximity malware, it will become immune towards the specific malware.

ECDSA process steps:

1. Create (dA) where dA is the private key of A.
2. If Party A authenticate as successful then computes K = (xK, yK) = dA.
3. The generated key is defined as xK and that key is passing from one application server to another.

Since it is practically impossible to find the private key dA from server transmission T, it is not possible for a third party to obtain the created key that passing in the sessions of different servers.

Evidence:

The evidence collection first specifies the real form of confirmation that every node have been conceptually referring. At each time interval set of nodes exchange their evidence based results which they own assessments on their neighbors with each other.

Evidence filtering:

In the evidence filtering scheme, there is an *initial setup* phase, during the period the system should collect a unique private key and public key which helps to the nodes to observe their neighbors.

Identifying Evil and Good Nodes using Evidences:

The system applies the ECDSA signature scheme for Node behavior identification.

Figure 1: Node behavior identification using the behavior and signature model Neighborhood Watch

In addition using a single node's own assessments, the node may include other neighbors' assessments in the cut-off decision against another node N. This extension to the evidence collection process is inspired by the real-life neighborhood watch program, which encourages residents to report suspicious criminal activities in their neighborhood.

Implementation

Implementation is the state where the theoretical design is converted into a working system. This state consists of Making necessary changes to the system as desired by the user.

- Training of the user personal prior to handle the system more effectively.
- Testing the developed programs with a sample data.
- Detection and correction of errors.

Experiment setup

Network construction

- ListNetworkComputer Namespace has been used to list out the system names, which are available in the network.
- A function for listing of all the PC's connected to the LAN is rendered by the network browser option. The formthis class with the help of a Dllimport instruction utilizes the listed collection of PC's. The aim for this is stated below,
- It is a call to C++ DLL, when a declaration of dllImport is made in managed code C#. These C++ Dll's used to carry out operations outside the managed code C# framework. These C++ dll's are a portion of either the operating system API or any vendors API.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

File transfer:

To transfer the encrypted files, the following techniques are used.

- Socket
- TCP Listener
- TCP Client
- Network Stream

1. First specify the destination IP/ System Name.
2. The IP and System Name can be retrieved from DNS(which provides Domain nameresoultion functionality)
3. TCP Listener listens for connections from TCP network clients.
4. TCP client Proides client connection for TCp networks.
5. Socket creates endpoint to the communication.
6. In the proposed model berkeley socket interface has been implemented.
7. For socket implementation the following parameteres should be used.

   a. Address family
   b. Socket type
   c. Protocol Type

Results and discussion

To evaluate the efficiency, four measures were used to evaluate the effectiveness. One is the number of modified entries, indicating how much the content of the original database is preserved. The other measures are defined as follows:

The following graph represents the time comparison between the existing and proposed systems. The results of these experiments are discussed

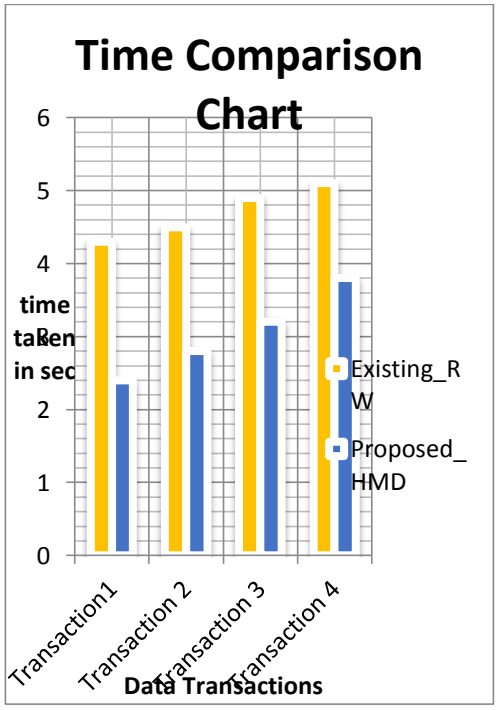
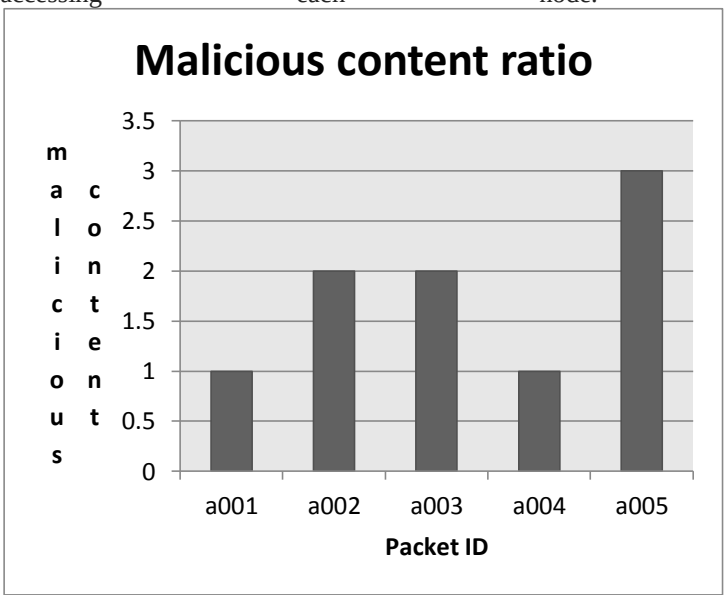


Chart1:comparison chart based on the time

The above chart represents time comparison graph between existing random waypoint technique and proposed HMD protocol. In this graph the existing technique takes 5 seconds to complete this process, and HMD completes by 3.5 seconds. Comparing with several existing technique the process of HMD algorithm is high, so that the processing time is reduced.

The next step is the analysis of probability calculation. This has been analyzed with the behavior of accessing each node.



ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Chart 2

The above chart represents the node transactional frequency which shows the amount of data transferred by every node. This helps to track and identify the probability of malware detection.

The above malicious content ratio Chart shows the probability of the nodes in order to find who has been inserted the malicious data. From this chart the malicious content in high in packeta005.

Conclusion

The proposed hybrid malware detection technique has successfully implemented to effectively identify and remove the malicious data in the data. The system utilizes the elliptic curve digital signature algorithm for secure evidence verification. The system overcomes the main three issues which are evidence collection risk and fake evidence identification and malicious code removal problem. The system also focused on the performance enhancement with two major metrics such as accuracy and detection time. To detection it use request - transmit and check scheme each node itself checks the number malicious code exists, and node carry the acknowledgement when they move, and cross-check if their carried claims are inconsistent when they contact. If node exceed the rate limit then declare the network contain flood attack. To avoid further transmission from attacker node put into the blacklist. No more than packets accept from attacker node. This mechanism effectively defends the malwares in DTN. The system performs an acknowledgement scheme to differentiate the attack types in DTN

Future work

The system may extend the malware detection work using other type of detection techniques such as game theory. The malware detection can be enhanced with the user specified rules for personalized opinion based malware filtering.In prospect; extension of the behavioral characterization of proximity malware to account for strategic malware detection evasion with game theory is a challenging yet interesting future work.

References

1. Peng, Wei, et al. "Behavioral Malware Detection in Delay Tolerant Networks."*Parallel and Distributed Systems, IEEE Transactions on* 25.1 (2014): 53-63.
2. Govindaraju, Aditya. "Exhaustive statistical analysis for detection of metamorphic malware." (2010).
3. Tahan, Gil, Lior Rokach, and Yuval Shahar. "Mal-id: Automatic malware detection using common segment analysis and meta-features." *The Journal of Machine Learning Research* 13.1 (2012): 949-979.
4. Mohaisen, Aziz, Omar Alrawi, and M. Larson. *AMAL: Highfidelity, behavior-based automated malware analysis and classification*. Verisign Labs, Tech. Rep, 2013.
5. Ramu, Srikanth. "Mobile Malware Evolution, Detection and Defense." *EECE 571B, TERM SURVEY PAPER* (2012).
6. Channakeshava, Karthik, et al. "High performance scalable and expressive modeling environment to study mobile malware in large dynamic networks."*Parallel & Distributed Processing Symposium (IPDPS), 2011 IEEE International*. IEEE, 2011.
7. Idika, Nwokedi, and Aditya P. Mathur. "A survey of malware detection techniques." *Purdue University* 48 (2007).