ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Behavioral Game and Signature Verification for Effective Malware Detection in DTN

B.Senthil Kumar[1], Dina Stephan K[2]

Assistant Professor, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[1]

M.Phil. Scholar, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India [2]

ABSTRACT: Delay tolerant network utilize the mobility of node and opportunistic contact among nodes for data communication. Due to this nature of DTNs, malware based attacks are increased tremendously. In modern network the malware is one of the life-threatening issues and it can be identified by many characters. Such character based issues are named as email spam, Denial of service and Trojan like viruses. Now a day's DTN (Delay Tolerant Network) is suffering from the above malware related issues. So defending those malware attacks using novel techniques is the main aim, of our proposed system. In order to thwart those attacks in DTN, our system introduces a new Hybrid Malware Detection and Removal technique in DTN named as HMDR. The proposed system deals with several malware detection issues and identifies the misbehaving nodes by collecting and validating their evidence using effective signature scheme. The hybrid malware detection and removal techniques analyses every node along with the behavioral score using behavioral game theory. The proposed system uses a hybrid malware detection and removal technique to find and remove the malware. In HMDR, each node in the DTN itself checks for the malware, and node carry the acknowledgement when they completes the verification, and signature will be appended if their verification is successful. If node exceeds the behavioural score then declare that the node is a malicious, this information will be disseminated to other nodes. To avoid further transmission from those nodes, HMDR put node information into the blacklist. No more than packets accept from attacker node. These are all the mechanisms effectively integrated against the malwares in DTN. The results show that the hybrid technique increases the efficiency and reduces the verification time.

KEYWORDS: Delay and Disruption Tolerant (DTN); Malware detection; malware removal, Game theory, signature schemes.

I. INTRODUCTION

Delay and Disruption Tolerant (DTN) is a new network architecture, which handles different technical issue in heterogeneous networks. DTN can improve communications by ensuring no information is lost even when a connection is interrupted. Such networks can improve communication in different remote applications such as military, disaster relief efforts and regions with limited communications infrastructure [1].

DTN can improve electronic communications by storing data when a connection is interrupted or disconnected. DTN overcomes those technical issues by forwarding it to its destination using relay stations. Due to this reliable nature, DTN affected by several attacks such as malware and malicious content injection issues. To defect and remove the malware, the proposed system utilizes a fusion based approach named as HMDR. In this proposal, we investigate the problem of improving the performance, security and scalability of DTN with effective behavior analysis, which could detect thousands of malwares based on its behaviors.

The main objectives of this paper are effectively identifying the proximity malware based attack in DTN using HMDR (Hybrid Malware Detection and removal) scheme. The current proposal aims at reducing the proof collection risk and insufficient evidence problem in the malware detection process. The system consists of the following additional objectives. Our system aims to implement a Fast and accurate malware detection with fusion of several behavior and signature based techniques. This also aims to compare and analyze the performance of different malware detection techniques in DTN with QOS metrics in terms of delivery probability and average delivery latency. In this study, we also study the impact of hybrid method on the performance of DTN under various security problems related to malware.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

II. RELATED WORK

In literature, there is several general malware detection methods have proposed. In such studies, pattern matching is the popular technique [2], which is a supervised learning process and data matching technique. However, the pattern matching technique is only successful when the malware detection used in common known networks. i.e. homogeneous networks. Later random waypoint method has been applied, recent findings on these techniques [3] [4] show that these models may not be realistic in DTN applications. Techniques from paper [5][6] designed on the observation that trust evaluations can link past experiences with future predictions. These techniques used reputation values and previous malfunction behavior for analysis.

In the malware detection background Dash et al [7] presented a distributed IDS architecture of local and global detector, which resembles the neighborhood-watch model, with the assumption of attested and honest evidence, without liars. In the neighborhood watch model, suspiciousness, defined in can be seen as nodes' reputation. To eliminate a node from the network the technique need to calculate whether it is trustworthy or not. So, the work [8] can be viewed from the perspective of reputation/trust systems. Some existing work expands the malware detection using Central authority, which is called the trusted third party. One global trust value is drawn and published for each node, based on other nodes' opinions of it. The above trust management systems allow each node to have its own view of other nodes. These are the works proposed to handle the malware in network.

.

III. PROPOSED ALGORITHM

Protecting a victim (host or network) from malicious behaviour is a hard problem that requires the coordination of several complementary mechanisms, together with nontechnical and technical solutions (at the application and/or network level). Several mechanisms have been proposed in the literature. So implementing malware detection and removal are very tedious because the network has so many vulnerabilities and security issues. The proposed system introduces a new technique which is named as HMDR (**Hybrid techniques for Malware Detection and Removal).** The decentralized approach provides effective rule matching and verification process to detect malware in the network while data transmission. Discretionary access control list has also applied in order to maintain black and white list of users and nodes for effective data restriction. The importance of the HMDR is facilitating a solution against filter selection problem.

- HMDR finds malwares in the content over DTN rapidly
- HMDR performs malicious data detection before transmitting the data.
- HMDR identifies the malware initiator machines, and informs to the other nodes about the malicious node.

The aim of the system is to effectively and efficiently detect malicious code at every hop. The proposed system optimally detects and eliminates malware using content tracking techniques, and this disseminates *a priori* knowledge about a particular malware group in the network to the neighbour nodes. The attacker can add malicious code while transmitting the data in the network. This is a challenging problem when end to end data verification. To overcome the problem, our proposal initiates and validates node behaviour by generating detection models based on behavioural game theory. Our system also executes and monitors an anti malware program in the data transmission environment. Based on these observations, our technique extracts the behaviour that characterizes the each node and its content over DTN. The behaviour is then automatically translated into detection and removal models that operate at very host in the network.

IV. PROPOSED METHODOLOGY

HMDR:

Our proposed system HMDR (**Hybrid Malware Detection and Removal) is a fusion based approach, which** combines the successful combination of **signature**, behavioural analysis using **behavioural game** and **pattern matching** techniques**.** Our approach provides an effective behavioural analysis and signature matching and neighbourhood verification process in the network at the time of data transmission. Consider a DTN consisting of n number of nodes in the network. The neighbours of a node are the nodes it has contact opportunities with. HMDR can effectively find the proximity malware in DTN, it is a malicious program, which interrupts the host node's normal function and has a chance of duplicating itself to other nodes during the contact opportunities between nodes in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

DTN. When duplication occurs in the network, the other node is infected with the malware. So detection of proximity malware is more important. The proposed system formulates the optimal signature based malware detection for proximity malware problem with the consideration of the heterogeneity of nodes and malware, and the limited resources of the defence system. The proposed model is suitable for both the MMS and proximity malware propagation. This utilizes a decentralized hybrid mixed algorithm for the signature distribution and effective malware detection. This proves that the proposed hybrid protection technique obtains the optimal solution for the system.

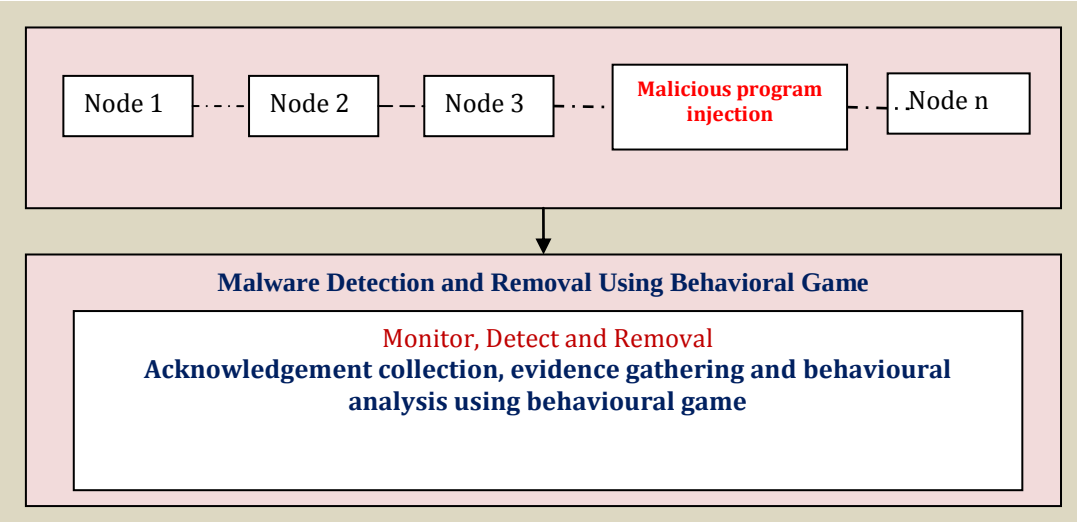

Fig 1.0 HMDR process

The proposed system introduces an acknowledgement scheme to disseminate the malware signatures along with the evidences (see fig 1.0). It only relies on local information and opportunistic contacts. The followings are the detailed description about HMDR process.

A. BEHAVIORAL GAME -BASED DETECTION

Behavioral game theory analyzes interactive deliberated decisions and behavior using the methods of game theory. In general, Traditional game theory focuses on mathematical equilibriums, rational choice and utility maximizing. But behavioral game theory concentrated on choices made by participants in studies and is game theory applied to experimentations. Behavioral game theory is a primarily positive theory instead of a normative theory. A positive theory is objective and based on evidences and positive theories must be testable and can be proven true or false. A normative theory is based on opinions and subjective in nature. Due to this nature, normative theories cannot be proven true or false in malware detection over DTN. Behavioral game theory attempts to explain decision making using experimental data, such as previous tested information's. So the HMDR uses behavioral game for identifying malicious nodes in the DTN.

a. Process:

Behavioral game based malware detection differs from the existing game theory methods, In that it identifies the action performed malware instead of identifying malware presence. The programs with dissimilar syntax's but having same behavior are collected, thus this single behavioral game signature can identify various samples of malware. These types of detection mechanisms helps in detecting the malwares which keeps on producing new type of malwares since they will always use the system resources and services in the similar manner. The behavioral game detector basically consists of following components which are as follows:

- **Data Collection:** This component collects the dynamic as well as static information's of nodes.
- **Analysis:** This component converts, the raw information collected by data collection component into intermediate depictions.
- **Matching Algorithm:** the matching algorithm component in behavioral game is used to compare the representation with the behavioral game signature.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

The functional assumption characterizes a malware infected node by the evaluations of its neighbors. If node i has N (pair wise) encounters with its neighbors and sN of them are estimated as suspicious by the neighbors, and its suspiciousness is defined as Si.

Behavioral games for malicious detection over DTN have the following steps.

In the following discussion, we investigate the decision process of a node i, which has k neighbors {n1; n2; . . . ; nk}, against a neighbor j; with no loss of generality, let j be n1. So, nodes are represented as {i, j, k, l …..n}.

Notations	Descriptions
n	node
P	Packets
Ack	acknowledgment
C	count of acknowledgements
t	threshold

Table 1.0 Algorithm Notations

The above table1.0 shows the notations and its descriptions used in the algorithm1. The following is the algorithm which used HMDR.

Algorithm 1: Behavioral games
Input: static and dynamic information of nodes
Output: Behavioral score.
Steps:

Step 1: for each node n {n1; n2; . . . ; nk},
Step 2: Collect the ack(n→P). Here P is represented as each packet.
Step 3: classify the ack into 3 types A, M, F (Where A as ACK, M as Malicious, F fake)
Step 4: count the acknowledgments ack of n.

$$S = \sum_{k=0}^{n} \binom{n}{k} P^k C^{n-k}$$

Step 5: if count of ack(n) > t then n is malicious
Step 6: else good node
Step 7: end

From the above behavioral game algorithm 1, each node's behavioral type will be analyzed. Using the trust score the nodes will be marked as evil node and stored in the black list.

After successful implementation of the above behavioral game algorithm, the HMDR process performs the acknowledgement collection process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. SIMULATION RESULTS

The system implements the proposed model using n number of nodes. To evaluate the performance of the techniques, the system has developed a visual studio.net framework environment.

Node id	Total packets transmitted	ACK	Malicious	Fake (fake acknowledgement)
A	120	110	6	4
B	90	27	13	50
C	23	22	1	0
D	41	41	0	0
E	56	50	5	1

Table 2.0 acknowledgements and its count for every transmitted packet

The above table 3.0 represents the experimental results of the HMDR with 5 nodes. The experiments have taken 5 nodes A, B, C, D, and E respectively. Total number of data packets sent by each node is traced and based on the acknowledgement the number of malicious and fake evidences are found.

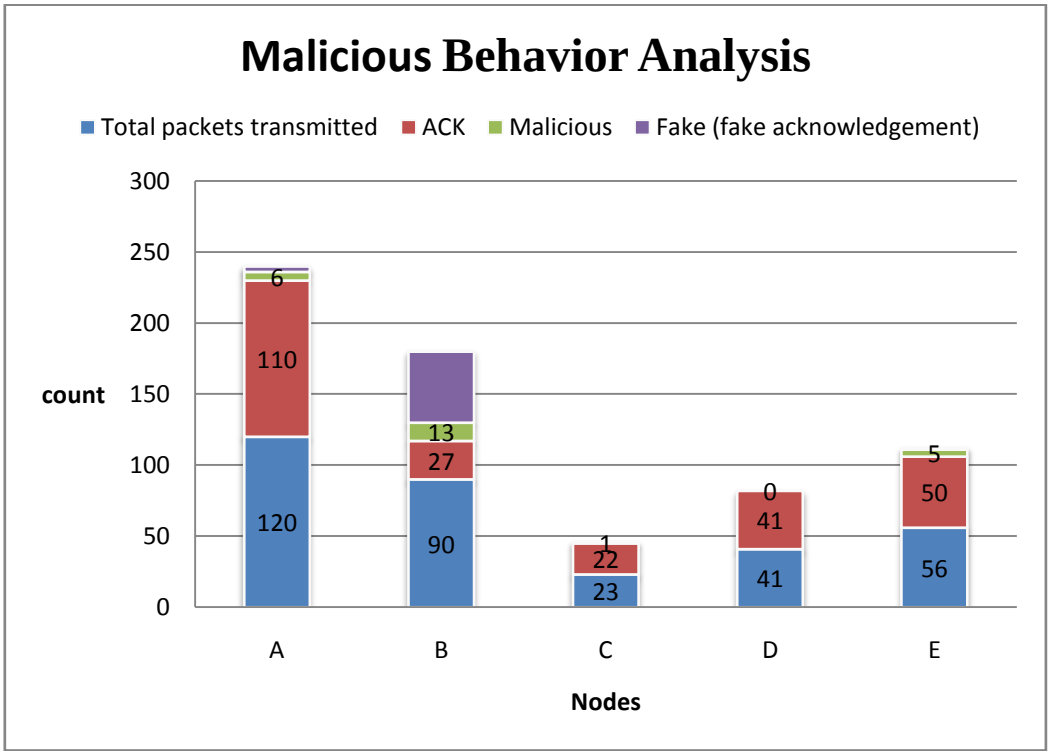

Fig2.0 malicious behaviour analysis using acknowledgments via behavioural game

The above table 2.0 and fig 2.0 shows the count of packets transmitted by every node and fake and malicious packet counts will be plotted respectively.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

	source	Intermediator	Dsetination	paths	malicious_score
1	N1	N2	N6	N1>N2>N6	88
2	N1	N3	N6	N1>N3>N6	89
3	N1	N4	N6	N1>N4>N6	91
4	N1	N6	N6	N1>N6>N6	92
5	N2	N1	N5	N2>N1>N5	76
6	N2	N3	N5	N2>N3>N5	79
7	N2	N4	N5	N2>N4>N5	81
8	N2	N6	N5	N2>N6>N5	83

Fig 3.0 Sample output of the above process

The above fig 3.0 shows a sample result from the experiment, from the figure, the malicious score of every node has been calculated according to the transaction.

V.RESULTS AND DISCUSSION

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

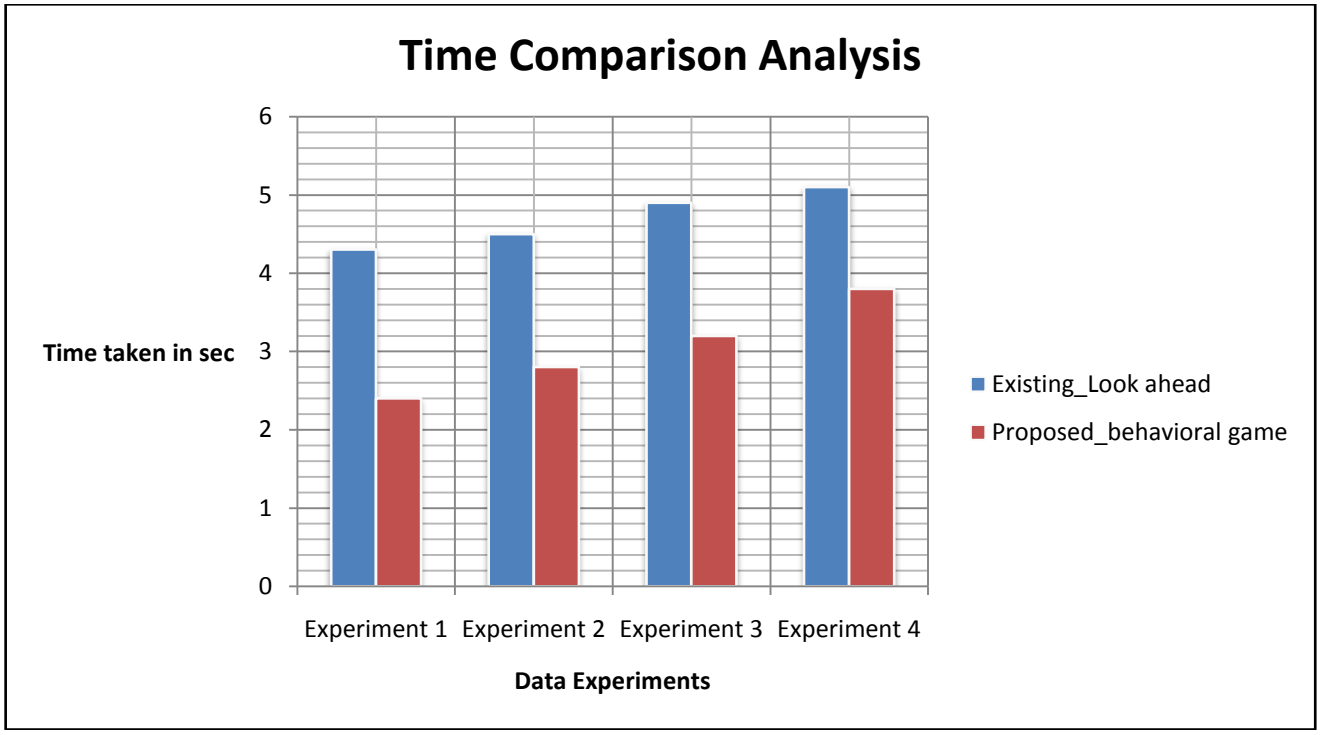

Fig 4.0 time comparison between existing look ahead method and proposed behavioral game method for malware detection

The above Figure 4.0 represents time comparison graph between existing random waypoint technique and proposed HMDR. In this graph the existing technique takes 5 seconds to complete this process, and HMDR completes by 3.5

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

seconds. Comparing with several existing technique the process of HMDR algorithm is high, so that the processing time is reduced.

VI. CONCLUSION

The proposed hybrid malware detection and removal technique with new behavioral game theory and signature algorithm are successfully implemented in DTN, The HMDR helps to effectively identify and remove the malicious data in the data before delivering it to the receiver. HMDR utilizes the elliptic curve digital signature algorithm for secure evidence verification. HMDR overcomes the main three issues which are evidence collection risk and fake evidence identification and malicious code removal problem. HMDR also focused on the performance enhancement with two major metrics. For effective malware detection we used a fusion based approach, which combines behavioural game, so each node itself checks the number malicious code and node carry the acknowledgement when the data transmission, and cross verification if nodes carried any other acknowledgments are inconsistent when they contact. If node exceed the score, then that is considered as evil node. To avoid further transmission from attacker node put into the blacklist. No more packets will accept from attacker node. Our proposed system effectively preserves the data from malware related attacks in DTN.

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] Panigrahi, Chhabi Rani, et al. "Malware Detection in Big Data Using Fast Pattern Matching: A Hadoop Based Comparison on GPU." *Mining Intelligence and Knowledge Exploration*. Springer International Publishing, 2014. 407-416.

[3] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling time-variant user mobility in wireless mobile networks," in Proc. IEEE INFOCOM, 2007

[4] Shahzamal, M., et al. "MOBILITY MODELS FOR DELAY TOLERANT NETWORK: ASurvey." *International Journal of Wireless & Mobile Networks* 6.4 (2014): 121.

[5] Chen, Ray, et al. "Trust management for encounter-based routing in delay tolerant networks." *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010.

[6] Peng, Wei, et al. "Behavioral detection and containment of proximity malware in delay tolerant networks." *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011.

[7] D. Dash, B. Kveton, J. Agosta, E. Schooler, J. Chandrashekar, A. Bachrach, and A. Newman, "When Gossip is Good: Distributed Probabilistic Inference for Detection of Slow Network Intrusions," Proc. 21st Nat'l Conf. Artificial Intelligence (AAAI), 2006.

[8] Lin, Yunfeng, Baochun Li, and Ben Liang. "Efficient network coded data transmissions in disruption tolerant networks." *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.