Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 244 – 251

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem

M.Poongodi*, S.Bose[a]

*Anna University,Chennai,India
[a]Anna University,Chennai,India

Abstract

The Detection and Prevention system against many attacks has been formulated in Mobile ad hoc networks to secure the data and to provide the uninterrupted service to the legitimate clients. The formulation of opinion of neighbors or belief value or Trust value plays vital role in the detection system to avoid attacks. The attack detection system always extracts the behaviors of nodes to identify the attack patterns and prediction of future attacks. The False positives and false negatives plays vital role on identification of attackers accurately without any false positives and negatives .Our system uses the Aumann agreement theorem for convergence of Truth on opinion based on the bound of confidence value , such that truth consensus will maintained, The accuracy of system will be enhanced through this methodology

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Keywords:Aumann agreement theorem , Truth of convergence , bound of confidence , detection system, Dual Trust Evaluation

1. Introduction

The bot net based attack is now familiar among many attackers to implement the DDoS attack easily. Many other tools are also available to implement the attack easily without any expertise in the tools. The need for the prevention and detection mechanism against DDoS attack is more necessary to avoid attacks as far as possible. Mobile ad hoc network is distributed wireless infrastructure less environment. There are wide applications of

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
*E-mail address:*author@institute.xxx

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.053

MANET in many fields (eg Military) etc. It is significant to defend against attacks on the MANET environment since it is used in very sensitive field of information sharing without any security. The Opinion formation model is given using Aumann Agreement theorem [3], the opinion is the probability of occurrence of attack by predicting the future through the Trust Value. The Trust value will be calculated according to the belief system and it is revealed by the members through the voting terminology. The Voting participants extract the behaviour of the neighbours by their traffic related information in order to provide uninterrupted service to the legitimated users by identifying the attackers in a fastest way . [4]The Vote participants can be chosen by hashing methodology by exchanging the routing information location , ID etc. The random selection of co-ordinates helps us to avoid the prior launching attacks on the target nodes[5][6]. The randomly selected vote participants such that votes for or against the target nodes securely by preloading the public/Private key pairs. The authenticity of vote is maintained by this preloaded key pairs. The Voting based on the Trust value is formulated by using the Traffic information, bound of confidence value is used to convergence towards the Truth, Such that identification of Attackers is fine tuned from Vote casting with the Aumann agreement theorem.

2. Literature Survey

[1]The prevention mechanism against the DDoS attack has been proposed. In this firecol updates the score through which the potential attack has been identified. Here DGSOT plays the vital role on clustering based on the score at the routing level. Such that secure aware routing of potential attack is possible.

[2]The node activity of network is monitored by using the location and time stamp. The message authentication code is used inaddition to identify the attack simulation in the network. The dropping of false data in the intermediate nodes before reaching the destination node, such that it can avoid the DDoS attack implemented by the attackers.

Pengrui Xia, Meng Wu, Kun Wang, Xi Chen et.al, [7] As the absence of a centralized control in mobile ad hoc networks (MANET), the tradition public key infrastructure (PKI) model is not fully applicable in MANET scenarios. Hence propose a fully distributed Certificate Authority (CA) which based the Identity-Based Encryption (IBE) combined with distributed secrete sharing algorithm and integrated it with an OLSR MANET

Jonathan Thostle.,[8] proposes a new concept in network addressing: one-time encrypted Network addresses. To tackle the two existing network security problems are ensuring anonymous communications and preventing data exfiltration through network covert channels. Author then show how one-time encrypted addresses can prevent intersection and other traffic analysis attacks that can undermine low-latency and anonymous communications

Tameem Eissa, Shukor Abd Razak, Md Asri Ngadi, et.al, [9] proposes a solution provides a safe way to use short cryptography keys for MANET. The system provides secrecy by hiding the public keys and making them visible only to the trusted nodes.

Yang Qin and Dijiang Huang [10].proposes a statistical traffic pattern discovery system (STPD). In brief, their approach includes three steps: (1) construct the point-to-point traffic matrices according to the captured packets and then derive the end-to-end (accumulative) traffic matrix; (2) compute the probability for each node to be a packet originator or a destination to distinguish the sources and destinations from forwarders; (3) the author deliberately erase the outgoing traffic from a source node or the incoming traffic to a destination node in step (1) and (2) to identify the end-to-end communication relations. The main contributions of this work are in two-fold: (i) improve the algorithms and present a new set of inference rules to construct the point-to-point traffic matrices and to derive the end-to-end traffic matrix more precisely. (ii) Upon the derived end-to-end traffic matrix, we propose a novel heuristic data processing model to derive the probability for each node to be a source or a destination, and the probability for each pair of nodes to be an end-to-end communication pair.

Suparna Biswas, Priyanka Dey.et.al, [11]. propose a check pointing–recovery scheme that eliminates much of these overheads. The contributions of the present work may be summarized as follows: A trust model is proposed that evaluates a MH to be trusted based on a number of parameters. A trusted cluster member MH is found out by a check pointing MH so that a copy of plain checkpoint could be saved in it. Secure check pointing using public key cryptography is used. The MH that saves checkpoint can access its content. A checkpoint is secure on a trusted MH.

Hence checkpoint can be sent to a trusted MH without encryption. Thus total energy consumption of MHs for receiving, forwarding encrypted checkpoint and channel bandwidth consumption to transmit it will reduce.

Jin-Hee Cho Æ Ing-Ray Chen [12], Investigate performance characteristics of secure group communication systems (GCSs) in mobile ad hoc networks that employ intrusion detection techniques for dealing with insider attacks tightly coupled with rekeying techniques for dealing the outsider attackers. The objective is to find the optimal settings with the the best intrusion detection interval and the best batch rekey interval under which the system lifetime (mean time to security failure) is maximized while satisfying performance requirements.

Feng Luo, Latifur Khan, Farokh Bastani, I-Ling Yen1 and Jizhong Zhou [13], the authors introduce a new hierarchical clustering algorithm that overcomes some of these drawbacks. A new tree-structured self-organizing network, called dynamically growing self-organizing tree (DGSOT) algorithm for hierarchical clustering. At each hierarchical level, the DGSOT contains the optimized number of clusters, from which the proper complete hierarchical structure of the underlying dataset can be found. In addition, they propose a new cluster validation criterion based on the geometric property of the Voronoi partition of the dataset in order to find the proper number of clusters at each hierarchical level. This uses the Minimum Spanning Tree (MST) concept of graph theory and it is computationally inexpensive for large number of datasets. A K -level up distribution (KLD) mechanism, which increases the data distribution in the hierarchy construction, which was used to improve the clustering accuracy. The mechanism of KLD allows the data misclustered in the early stages to be re-evaluated at a later stage and increases the accuracy of the final clustering result. The clustering result of the dynamically growing self organizing tree is easily displayed as a dendrogram for visualization.

Dmitri D. Perkins, Herman D. Hughes, and Charles B. Owen,[14] Mobile Ad Hoc NETworks (MANETs) are an emerging class of network architectures that are characterized by their highly dynamic topology, limited resources bandwidth ,power, and lack of fixed infrastructure. The motivation for such networks is increased mobility with the flexibility. Random node mobility along with various other factors such as network size and traffic intensity may be very dynamic, resulting in unpredictable variations for the overall network performance. The modelling and development of adaptive ad hoc protocols (routing, medium access control, scheduling and buffer management).Using 2kr factorial experimental design, which isolates and quantify the effects of five factors: node network size, number of traffic sources, and type of routing (source versus distributed), that affects the performance of mobile ad hoc networks.

3. Proposed System

3.1Trust Evaluation System

The process involves estimating the trust value of all the nodes of a network. Based on the trust value characteristics, we eliminate the affected nodes. Rekeying protocols are used to provide confidentiality and secrecy. Regular rekeying is performed, and the group keys are generated time from time for all the nodes. This is vital for ensuring the security of the network. We use Direct Trust Observation Model to calculate the trust value of a particular node. It is recursive in nature, thereby making it easy to compute future trust values. After calculating trust values, we use the Voting based IDS system to distinguish compromised nodes from uncompromised nodes. This system will help us to identify normal nodes along with malicious nodes. Aumann Agreement theorem is used to calculate the truth and confidence values of nodes in the network and then group them into two distinct groups, each group communicating with each other. The bound separating them is called as Bound of Confidence Value and this is in turn used to converge to the truth. Dual Weighted Trust formula is used to update the trust values based on the behavior characteristics of the node in the network. More the degree of compromise, lower the trust value, and vice versa. Also, rekeying protocols are used to provide confidentiality and secrecy. This is important to ensure the stability and security of the network. Together, we determine the trust values of all the nodes in a network, and if the trust values are abnormal, we eliminate the suspicious node from the network.

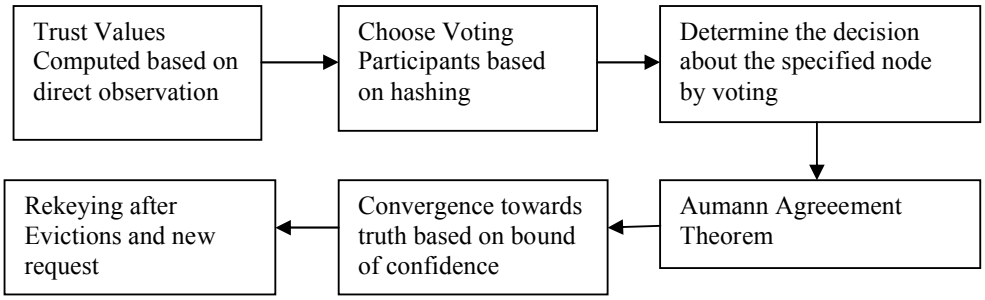

Fig 1: System Architecture

3.2 Direct Trust Observation Model

The trust value is derived using Bayesian inference, which is a type of uncertain reasoning. Trust value in the model by a real number with a continuous value between 0 and 1. We evaluate trust values with direct observation on the malicious behavior characteristics and packet dropping.
Now let us assume that

- ***x*** is the number of packets can be forwarded,
- ***y*** is the number of packets sent by a node.

$$TS = \alpha_n / \alpha_n + \beta_n$$

Where

Ts = trust value of the nodes

$\alpha_n = \alpha_{n-1} + x_{n-1}$

$\beta_n = \beta_{n-1} + yn\text{-}1 - x_{n-1}$

And $\alpha_0 = 1$, $\beta_0 = 1$

The trust value of a node is 0.5 at the beginning. This means that the node is neutral with no history of behaviors Established.

3.3 Voting based IDS

Under Voting based IDS whether target node is compromised or uncompromised is detected based on voting. Periodically a node, called a target node, would be evaluated by m vote-participants selected by hash function. If the participants decided to vote against or for the target node, then two groups consisting of these nodes are created based on their votes. Co-ordinator is selected randomly who selects the members for voting. The voting participants should have communicated with the target node and it should be of odd number. Let m be the number of nodes being selected for voting from communicated group based on Hashing.

V- **group containing the list of m voters**
V- { 1, 2, 3, ... m }
Mod value is selected randomly by Co-ordinator for hashing.
Hashing = mod function

Pnode i(TN) = Ti ;
where i - participant is in the voter's list
Ti – Trust value of the ith node for Target Node(TN)

IF Ti >= Th it indicates the group of nodes casting vote for TN as uncompromised (G1)
ELSE
it indicates the group of nodes casting vote for TN as compromised (G2)

Th – Threshold (0.5 is value because neutral nodes trust value is 0.5)

3.4 Aumann Agreement Theorem

Communication is performed between the two group of nodes. The Bound of Confidence value is primarily used to converge the nodes to truth. The Aumann's theorem now says that majority of nodes may converge into truth(compromised or not).

G1 = { group of nodes casting vote as uncompromised node }
G2 = { group of nodes casting vote as compromised node }

After the nodes are placed in seperate groups,the nodes in two groups communicate with each other. Now the **bound of confidence** value is now used to determine the truth value. **| Threshold - Pnode i(TN) | < 0.1** [In this case] Then move the nodes with this small marginal value to the other group so that they are being converged into a truth consensus.

3.5 Dual Weighted Trust

The decision parameter (DTN) of the node is used to determine and verify the decision by the nodes. Based on this decision, the node can be eliminated. In detecting malicious nodes, we employ decision to update the trust values of nodes in decision making process. The decision parameter is used to determine and verify the decision by the nodes so that the node can be eliminated or not.

If G1 > G2
D_{TN} = Total no of nodes in G1 / Total no of nodes participated
Else
D_{TN} = Total no of nodes in G2 / Total no of nodes participated

Hence we obtain the decision of the nodes and mark the node as compromised or uncompromised. When D_{TN}< 0.5, the trust values Ti(v) of G2 is increased and G1 is decreased. When D_{TN}> 0.5, the trust values Ti(v) of G1 is increased and G2 is decreased. If the trust value of the specified node has not been obtained (or) if the node has not involved in any communication, its trust value is taken as 1.

If D_{TN}> 0.5
Ti(v) = max (Ti(v)– Θ , 0) for K != G1
Ti(v) = min (Ti(v)+ Θ , 1) for K = G1

Else
Ti(v) = max (Ti(v) – Θ , 0) for K = G2
Ti(v) = min (Ti(v) + Θ , 1) for K != G2

Θ – Penalty ranging between 0 and 1.

Now the trust values for nodes that has cast votes based on truth will be increased and the other group will be reduced Now the node which has trust value nearer or less than 0 is the malicious node being detected and is evicted from the system. MTTSF(Mean Time to Security Failure) indicates the time interval the system operates normally before it experiences any failure.

3.6 Rekeying

During rekeying phase the regeneration of group key obtained messages from one of its member whenever membership update needed. The communication happens securely between the cluster heads, wherein the network head generates the key and passes on among the cluster leaders. If no member exists in the tree, then create a new tree T with the new node If members exist, then nodes are being inserted in the tree, the rightmost node being chosen as sponsor. Rekeying is performed only when nodes exit and enter the system with the existence of the sponsor and R_N value is met.

4. Results And Discussion

The Experimental analysis of our proposed system is done with NS 2 simulator for 200 nodes and evaluated the Parameters Detection rate , Packet delivery ratio with existing IDS techniques for DDoS attack in MANET.

The Evaluation proved that proposed system gives better security and increased performance of the network comparatively.The Comparison algorithm FC-DGSOT,Co-operative authentication scheme which are specified in the literature.[1] and [2]

Table 1: Simulation Environment

Simulation Environment	**Simulation Value**
Wireless standard	IEEE 802.11
Number of nodes	200
Base Routing protocol	AODV
Algorithm	Dual Weighted Trust
System Bandwidth	2 Mbps
Simulation Environment	1500 * 1500
Antenna	Omni Directional
Channel Propagation	Wireless / Two ray ground

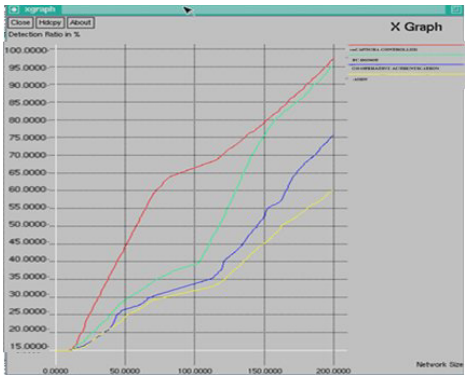

Figure 2:Detection rate

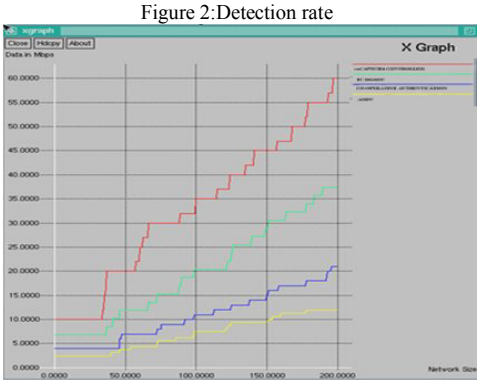

Figure 3: Packet Delivery ratio

Proposed system
FC-DGSOT
Firecol
Normal-AODV

5. Conclusion:

The Trustfulness and bound of confidence provides the duality trust to achieve the accurate results on malicious activities of node. Such that the security of the system is very high. Aumann agreement theorem can be applied for truthfulness against the any sensitive system to acquire accurate results. As a future work, the trust evaluation with bound of confidence in the multi-relay access network with heterogeneous environment can be proposed and the comparative results can be analyzed.

Reference

[1] Poongodi, M., and S. Bose. "Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFC in collaborative protection networks."*Advanced Computing (ICoAC), 2013 Fifth International Conference on*. IEEE, 2013.

[2] Poongodi M.(Manoharan), Bose.S, N.Ganesh kumar ." The Effective Intrusion Detection System Using Optimal Feature Selection Algorithm . "*International journal of Enterprise network management*",Forth Coming issue 2015 http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijenm

[3] Aumann, Robert J. "Agreeing to disagree." *The annals of statistics* (1976): 1236-1239.

[4] Cho, Jin-Hee, and Ing-Ray Chen. "Modeling and analysis of intrusion detection integrated with batch rekeying for dynamic group communication systems in mobile ad hoc networks." *Wireless Networks* 16.4 (2010): 1157-1173.

[5] Lang, R., & Deng, Z.."Data distribution algorithm using time based weighted distributed hash tables. Proceedings of 7th International Conference on Grid and Cooperative Computing" (pp. 210–213), 24–26 Oct 2008.

[6] Zhang, H., Goel, A., & Govindan, R. " Improving lookup latency in distributed hash table systems using random sampling". IEEE/ACM Transactions on Networking, 13(5), 1121–1134.

[7]. Pengrui Xia, Meng Wu, Kun Wang ,Xi Chen, " Identity-based Fully Distributed Certificate Authority in an OLSR MANET". Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on 12-14 Oct. 2008 Pg.no 1-4.

[8]. Jonathan Thostle, "Applying Network Address Encryption to Anonymity And Preventing Data Exfiltration." Military Communications Conference, 2008. MILCOM 2008. IEEE 2008 , Page(s): 1- 7.

[9]. Tameem Eissa, Shukor Abd Razak, Md Asri Ngadi, " Enhancing MANET Security using Secret Public Keys" International Conference on Future Networks 2009,page(s):130-134.

[10] Yang Qin and Dijiang Huang, "A Statistical Traffic Pattern Discovery System for MANETs" , Dependable and Secure Computing, IEEE Transactions on 2014 Volume: 11, Issue: 2 , Page(s): 181- 192.

[11]. Suparna Biswas, Priyanka Dey," Secure Check pointing-Recovery using Trusted Nodes in MANET", 4th International Conference on Computer and Communication Technology 2013, page(s): 175-180.

[12] Jin-Hee Cho Æ Ing-Ray Chen "Modelling And Analysis Of Intrusion Detection Integrated With Batch Rekeying For Dynamic Group Communication Systems In Mobile Ad Hoc Networks" in Wireless Netw (2010) 16:Pg.no 1157–1173.

[13] Feng Luo, Latifur Khan, Farokh Bastani, I-Ling Yen and Jizhong Zhou."A dynamically growing self-organizing tree (DGSOT) for hierarchical clustering gene expression profiles" Bioinformatics 2004 volume 20.page(s):2605-2617.30

[14] Perkins D.D "Factors Affecting the Performance of Ad Hoc Networks", IEEE International conference on communications 2002 volume 4,pages:2048-2052

[15]Zhexiong Wei, Helen Tang, Member, IEEE, F. Richard Yu, Senior Member, IEEE, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Conference Publications, November 2014

[16]Jin-Hee Cho, Ing-Ray Chen, "Modeling and analysis of intrusion detection integrated with batch rekeying for dynamic group communication systems in mobile ad hoc networks", IEEE Wireless Networks 16, July 2010.

[17]Yaser Khamayseh, Ruba Al-Salah, Muneer Bani Yassein, "Malicious Nodes Detection in MANETs," Proc. IEEE International Advanced Computing Conference, 2012.

[18] Lorenz Demey, Prof Dr Dick de Jongh, "Agreeing to Disagree in Probabilistic Dynamic Epistemic Logic," Proc. IEEE NETWORK, September, 2010

[19] Poongodi.M and S.Bose "The COLLID Based Intrusion Detection System for Detection against DDOS Attacks using Trust Evaluation . " Advances in Natural and Applied science", 9(6) Special 2015, Pages: 574-580