Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 12, pp. 22716-22720, December, 2017

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

AN ENERGY EFFICIENT INTRUSION PREVENTION SYSTEM USING TRUST MANAGEMENT APPROACHES IN WIRELESS SENSOR NETWORK

Perumal V and Meenakshi Sundaram K

Department of Computer Science, Erode Arts & Science College (Autonomous),
Erode, Tamilnadu, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0812.1323

ARTICLE INFO

Article History:

Received 15th September, 2017
Received in revised form 25th October, 2017
Accepted 23rd November, 2017
Published online 28th December, 2017

Key Words:

IPS, IDS, Trust Management.

ABSTRACT

Intrusion Prevention Systems (IPS) are deployed in-line with the network segment being protected. All data that flows between the protected segment and the rest of the network must pass through the NIPS. As the traffic passes through the IPS, it is inspected for the presence of an attack. Like viruses, most intruder activities have some sort of signatures. A growing number of Sensor and Ad-hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors for improving the securities in any network environment. However, such a process can be easily abused or disrupted by adversarial nodes. In absence of a-priority trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature. Trust Management Approaches and clustering based approaches are used to reduce the false rejection ratio in mobile nodes and agents. First identify the trusted nodes in networks, then packets will send through that trusted nodes. Trusted nodes are identified based on trust values for identify the neighboring nodes for verification process for improving the Packet Delivery Ratio and Energy Consumption.

INTRODUCTION

Intrusion Prevention Systems are designed to protect information systems from unauthorized access, damage or disruption. Vendors have developed IPS to counteract the rapidly evolving threats presented by the latest generation of worms, software and network exploits. As the number and frequency of threats has increased, the increasing complexity of the network environment has made mitigation of these threats harder to achieve. Modern networks have evolved for the purposes of distributing critical information and services to an ever-expanding group of users.

The need for access to these critical services has led to the development of redundant communication links, wireless networks, mobile notebook computers, handheld digital devices, even internet-enabled cellular phones. These new access technologies and links increase the value of the information systems they support, but at the same time provide more paths for attack and compromise. This work will address the need for Intrusion Prevention Systems.

The need for IPS

Intrusion Detection Systems (IDS) were developed to identify and report attacks to corporate Security personnel for manual remediation. Traditional Intrusion Detection technologies do nothing to stop an attack they simply detect hostile traffic and send alerts. As the level of threats and the size of IDS deployments increased, it was found that the amount of time needed to analyze and respond to the IDS systems was becoming prohibitively large.

The evolution of new hybrid attacks that use multiple vectors to breech the security infrastructure highlighted the need for the enterprise to defend itself against a constantly shifting threat. Organizations have suffered catastrophic damage to their business confidentiality, integrity and availability as intrusions have become more virulent.

Functions of IPS

IPS Functions is to identify the malicious activity, Log information related to such activity, Attempt to block / stop such activity and Report the activity.

Corresponding author:* **Perumal V
Department of Computer Science, Erode Arts & Science College (Autonomous), Erode, Tamilnadu, India

Network IPS

A software or dedicated hardware system that connects directly to a network segment and protects all of the systems attached to the same or downstream network segments. Network IPS devices are deployed in-line with the network segment being protected. All data that flows between the protected segment and the rest of the network must pass through the Network IPS device. As the traffic passes through the device, it is inspected for the presence of an attack. Attack detection mechanisms vary between systems, but the most accurate systems integrate several techniques to achieve very high levels of confidence in the detection of attacks and misuse.

Extreme accuracy and high levels of performance are crucial to an effective system as mis-identification of an attack can cause legitimate traffic to be blocked, which would be, in essence a self-inflicted "Denial of Service" condition. High performance is necessary to ensure that legitimate traffic is not delayed or disrupted as it flows through the device. When an attack is identified, the Network IPS discards or blocks the offending data from passing through the system to the intended victim thus blocking the attack.

Trust Management

Trust in general is the level of confidence in a person or a thing. Various engineering models such as security, usability, reliability, availability, safety, and privacy models incorporate some limited aspects of trust with different meanings. For example, in sensor network security, trust is a level of assurance about a key's authenticity that would be provided by some centralized trusted body to the sensor node (SN). We consider two types of trust properties:

QoS trust: QoS trust is evaluated through to the communication network by the capability of a node to deliver messages to the destination node. We consider connectivity and energy to measure the QoS trust level of a node.

Social trust: Social trust is based on honesty or integrity in social relationships and friendship in social ties. We consider healthiness and social unselfishness to measure the social trust level of a node. The healthiness social trust is the belief of whether a node is malicious.

A number of trust management schemes have been proposed for peer-to-peer networks and ad hoc networks. To the best of our knowledge, very few comprehensive trust management schemes (e.g., Reputation-based Framework for Sensor Networks (RFSN), Agent-based Trust and Reputation Management (ATRM), and Parameterized and Localized trust management Scheme (PLUS) have been proposed for sensor networks.

There are two topologies: Intra-group topology where distributed trust management approach is used and intergroup topology where centralized trust management approach is adopted. This methodology helps to drastically reduce the cost associated with trust evaluation of distant nodes. For the Intra-group network, each sensor that is a member of the group calculates individual trust values for all group members.

Based on the trust values, a node assigns one of the three possible states. They are Trusted, Untrusted and Uncertain to other member nodes. This three-state solution is chosen for mathematical simplicity and is found to provide appropriate granularity to cover the situation. After that, each node forwards the trust state of all the group member nodes to the CH. Then, centralized trust management takes over.

METHODOLOGY

The existing methodology and the proposed methodology which employed to provide an efficient methods and technique that aims to achieve the objectives of this research. The Implementation phase is a stage in the system where the theoretical design turned into working system. The most critical stage is the user confidence that the new system will work effectively and efficiently.

Existing Work

The Existing method have designed and implemented a full NIPS system that is based on a novel pattern matching algorithm, called TCAM. We have shown that our solution is adequate for NIPS device developers, as it achieves line-speed rates. Specifically, for about 60% of real network traffic, an average line speed of 12*.35* Gbps can be achieved. This work presents several major advantages over existing NIPS devices. First, the achieved line-rate speed is several orders of magnitude faster than related works. Second, as opposed to other solutions, our system is fully compatible with Snort's rules syntax. Using TCAM algorithm Intrusion is prevented with help of NIPS data set. Here using hardware intrusion prevention is implemented.

Ternary Content Addressable Memory (TCAM)

The patterns list data structure is accessed in TCAM algorithm. A patterns list entry contains several fields which hold the information needed to implement the various Snort keywords: *Len* - is the pattern's length; *root* - is a Boolean that indicates whether this pattern is the first pattern of a rule; *offset* - indicates from where in the packet the pattern should be searched; *distance* - the minimum number of bytes allowed between two successive matches *within* – the maximum number of bytes allowed between two successive pattern matches; *depth* - how far into the packet the algorithm should search for the specified pattern; *TCAM Pars* - an array of TCAM references that are used in the algorithm whenever the pattern's length is greater than *w*. TCAM Rules table correlates between a TCAM row and the patterns list. Each table entry contains the shift value, an inclusion patterns list and a list of associated patterns.

Matched Patterns List holds the matched patterns for the current processed packet. Each entry contains the matched patterns and their corresponding end position in the packet. The rules list maps between a single rule and its corresponding patterns. Each entry contains the number of patterns in the rule, and a bitmap with a bit for each pattern. The existing TCAM pattern matching algorithm shows given below,

Drawbacks of the Existing System

The main drawbacks of the existing system are, does not consider False Rejection Ratio of IPS and does not consider Trusting Evaluation for every node.

```
Step 1: Define Packet T= {Ti,1 ≤ i ≤ n}
Step 2: IF position is1, then shift =0 while position ≤   to the   difference of n and
    width then   for the key packet(T)  position is  position + width −1]
Step 3: Enter the TCAM. Lookup (key)
Step 4: IF enter the entry and shift, for IF statement shift is   not   equal to 0 then
    position is position + shift then end the IF statement
Step 5: To begin the For statement for all current node enter   the Pattern Node.
    next = null ,if current length is  ≤ width OR check Sub Patterns is True then
    Matched List is add(current) and then end the all statement.
Step 6: Check the Sub-Patterns (length, position, TCAM Pointers)
Step 7: Repeat Step 2 and 3
Step 8: If enter the entry and shift is not equal to 0 or entry.id is TCAM Pointers ,
    then return false  for the IF statement, return true for the WHILE statement
```

Proposed Work

In this work we use Intra-group network. For the Intra-group network, each sensor that is a member of the group calculates individual trust values for all group members. Based on the trust states of all group members, a CH detects the malicious node(s) and forwards a report to the BS. On request, each CH also sends trust values of other CHs to the BS. Once this information reaches the BS, it assigns one of the three possible states to the whole group. They are Trust calculation at the node level, Trust calculation at the cluster-head level and Trust calculation at the BS level.

GBTM calculates the trust value based on direct or indirect observations. Direct observations represent the number of successful and unsuccessful interaction, indirect observations represent the recommendations of trusted peers about a specific node. Here, interaction means the cooperation of two nodes. For example, a sender will consider an interaction as successful if the sender receives an assurance that the packet is successfully received by the neighbor node and that node has forwarded the packet toward the destination in an unaltered fashion.

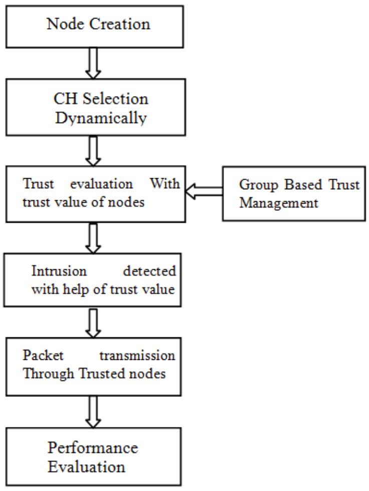
Node Creation
CH Selection Dynamically
Trust evaluation With trust value of nodes
Group Based Trust Management
Intrusion detected with help of trust value
Packet transmission Through Trusted nodes
Performance Evaluation

Fig 1 Proposed Model

In Fig 1, the wireless sensor network with 50 nodes is created in the NS-2.34 version. An energy model is used to calculate the energy of each node. Now the energy calculated for the nodes is compared with one another and the node with higher energy is found. This node with higher node energy is assumed as the cluster head. At the next step the trust values of the 50 nodes are calculated considering the successful and unsuccessful transmissions. If the trust value of the node is 2 then the node is trusted node. If the trust value is other than 2, then the nodes are considered untrusted according to the Group based trust management scheme.

The proposed Group Based Trust Management Algorithm shows given below,

```
Step 1:  Network nodes creation
Step 2:  CH selection based on dynamic ( because of selection   of
    source )
Step 3:  Trust evaluation process
Step 4:  Identify the Trusted nodes and intruder nodes ( malicious
    nodes ) or untrusted nodes
Step 5:  Secure communication
Step 6:  Performance analysis
```

Trust Calculation at the Cluster-Head Level

Assume that the CH is the SN that has higher computational power and memory as compared to other SNs.

Trust State Calculation of Intra Group

In order to calculate the global trust value of nodes in a group, CH asks the nodes for their trust states of other members in the group. We use the trust states instead of the exact trust values due to two reasons. First, the communication overhead would be less as only a simple state is to be forwarded to the CH. Second, the trust boundaries of an individual node vary from other nodes. In response, all group member nodes forward their trust states, s, of other member nodes to the CH. The variable, s can take three possible states: trusted, uncertain, and untrusted. The CH will maintain these trust states in a matrix form, as shown below

$$T\,Mch = \begin{array}{cccc} sch,1 & s1,c & \dots & sn,1 \\ sch,2 & s1{,}2 & \dots & sn,2 \\ \vdots & \vdots & & \vdots \end{array}$$

Where T Mch represents the trust state matrix of cluster head ch, and sch, 1 represents the state of node 1 at cluster head ch. The CH assigns a global trust state to a node based on the relative difference in trust states for that node. We emulate this relative difference through a standard normal distribution. Therefore, the CH will define a random variable X such that

2, when trusted

Trust value of the node = 1, when uncertain

0, when untrusted

Assuming this to be a uniform random variable, we define the sum of m such random variables as Sm. The behavior of Sm will be that of a normal variable due to the central limit theorem. The expected value of this random variable is m and the standard deviation $\sqrt{\ } m/$ The CH defines the following standard normal random variable for a node j,

$$Z_j = \frac{\sqrt{3\left(X\left(S_{ch,j}\right) + \sum_{i=1,i\neq j}^{m} X\left(S_{ch,j}\right) - m\right)}}{\sqrt{m}}$$

If $Z_j \epsilon$ [-1, 1], then node j is termed as uncertain, else if $Z_j > 1$, it is called trusted. If $Z_j < -1$, it is labeled as untrusted.

RESULTS AND DISCUSSION

The experimental results are compared with existing TCAM Algorithm. The GBTM technique is implemented on a Network setup which consists of 20 nodes including the intruder node. The NS2 tool is used to validate these techniques.

The TCAM Techniques for only increase line rate speed and for the Transmission. The trusted nodes are found and their node color is changed. After finding the trusted nodes the transmission between the trusted nodes occurs and finally the packets are transmitted to the cluster head. In order to overcome this problem, GBTM Technique is proposed to detect and prevent the Intrusion used to trust evaluation for neighbour node and the results are discussed in the following sections.

Parameters for Comparisons

The existing and proposed techniques are compared in terms of two metrics namely, Packet Delivery Ratio, Energy Consumption. These two parameters are compared TCAM and proposed GBTM Technique deployment and the findings are depicted through graphs.

Packet Delivery Ratio

The number of packets sent per unit time is called throughput (packet delivery). The first validation with respect to the Packet delivery Ratio measurement between the TCAM and the proposed GBTM techniques. The packets transmission time is taken in X axis. And the number of packets delivery is taken in Y axis. In both the existing and the proposed techniques, packet delivery is found to be increased. In the GBTM technique, the trust value of every node is an additional procedure to be followed by the network. This shows that GBTM technique performs well with making increased of packet delivery ratio.

Table 1 Performance Analysis based *on Packet Delivery Ratio*

Time (ms)	TCAM	GBTM
10	65	70
20	125	135
30	200	210
40	250	275
50	330	360

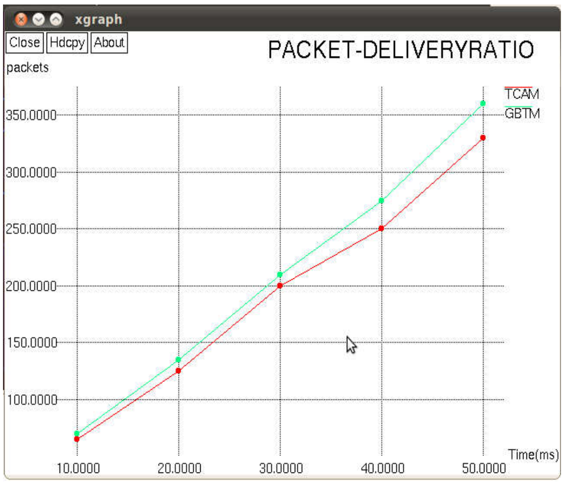

Fig 1 Packet Delivery Ratio Comparisons

From the figure 1 shows that Packet Delivery Ratio with respect to transmission time. This shows that GBTM technique performs well with making increased of packet Delivery ratio.

Energy Consumption

The second parameter to validate the proposed technique is energy consumption. The energy consumption is the energy loss taken to transmissions of Packets. In the proposed GBTM technique, the energy consumption is found to be reduced as shown in below table 2.

Table 2 Performance Analysis based on Energy Consumption

Packets	TCAM (%)	GBTM (%)
100	46.3	41.9
200	55.5	50.3
300	64.2	56.7
400	69.6	64.4
500	77.8	70.5

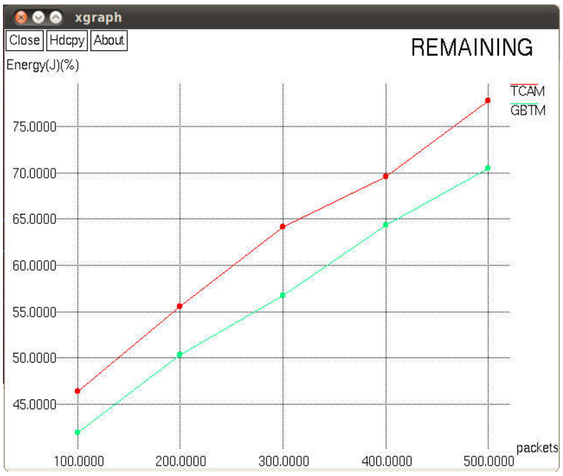

Fig 2 Energy Consumption Comparisons

From the figure 2 the Energy Consumption for the proposed Technique GBTM is reduced compared with the existing TCAM technique. Energy Consumption is reduced approximately 5% to 8%. Since, Energy Consumption is reduced, traffic becomes faster for the legitimate users. In this research work, both the existing and the proposed techniques are tested on the Network setup.

Performance Analysis

The performance of the GBTM Technique in the Intrusion Prevention System is greater when compared to TCAM Technique Performance is calculate by using, Packet Delivery Ratio and Energy Consumption. The performance analysis comparison table is shown in below table 3

Table 3 Performance Analysis

Methods	Performance (%)
TCAM	60
GBTM	75

CONCLUSION

Security is most important issues in wireless network. Using our proposed approach, trust management protocol is used to identify the trusted nodes with malicious node directions for efficient and secure communication in any kind networks. Our approach is to dynamically create the cluster heads based on energy profile on each and every node and to validate a group-based trust management scheme for secure routing for optimization in sensor networks.

The simulation results show that our scheme demands less energy consumption and energy dissipation as compared with the dynamic trust-based management schemes and it is secure for routing in wireless sensor networks. Finally we conclude that our proposed technique GBTM gives better performance in evaluating in parameters, Packet Delivery Ratio and Energy Consumption.

References

1. P. Albers, O. Camp, J. Percher, B. Jouga, and R. Puttini, “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches”, Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12April 2002.
2. I. R. Chen, F. Bao, M. Chang, and J. H. Cho, “Supplemental Material for 'Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing”, IEEE Transactions on Parallel and Distributed Systems, 2013.
3. Chong Eik Loo Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami, “Intrusion Detection for Routing Attacks in Sensor Networks”,2011.
4. David R. Musser and Gor V. Nishanov, “A fast generic sequence matching algorithm”, May 13 2000.
5. E. Guillen, D. Padilla, and Y. Colorado, “based Intrusion Detection and Prevention Systems”, Latin-American Conference Communications, pp.1-4, 2009.
6. Ing-Ray Chen, FenyeBao, MoonJeong Chang, and Jin-Hee Cho, “Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing”, IEEE Transactions on Parallel and Distributed Systems, May 2013.
7. Ms.B.Lakshmi, Mr.R.Karthikeyan, “Detection and Prevention of Impersonation Attack in Wireless networks”, *International Journal of Advanced Research in Computer Science & Technology* (IJARCST 2014).
8. E.E. Schultz and E. Ray, “Future of Intrusion Prevention”, Computer Fraud & Security, 2007, pp. 11-13.
9. S. Trifunovic, F. Legendre, and C. Anastasiades, “Social Trust in Opportunistic Networks”, IEEE Conference on Computer Communications Workshops, San Diego, CA, USA, March 2010.
10. Varsha Nigam, Saurabh Jain “An Efficient Modular Approach of Intrusion Prevention in Wireless Sensor Networks”, International Journal of Recent Technology and Engineering (IJRTE), 2013.
11. Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM/Kluwer Wireless Networks Journal (ACM WINET), vol. 9, no. 5, September 2003.
12. Nabil Ali Alrajeh, S. Khan, and Bilal Shams, “Intrusion Detection Systems in Wireless Sensor Networks”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks vol.13, Article ID 167575, pp.1-7, 2013.
13. G. Marmol and G.M. Perez, “Security threats scenarios in trust and reputation models for distributed systems”, Computers & Security, vol. 28, pp. 545-556, 2009.
14. S. Trifunovic, F. Legendre, and C. Anastasiades, “Social Trust in Opportunistic Networks”, IEEE Conference on Computer Communications Workshops, San Diego, CA, USA, March 2010.
15. Mansoor Alicheery, Vijay Kumar, Muthuprassana," A High Speed Pattern Matching for Network IDS/IPS", vol.1, pp.187-196, 2006.
16. Chris Karlof, David Wagner “Secure routing in Wireless Sensor Networks: attacks and countermeasures” Elsevier, vol-1, pp (293-315), 2003.

How to cite this article:

Perumal V and Meenakshi Sundaram K.2017, An Energy Efficient Intrusion Prevention System Using Trust Management Approaches In Wireless Sensor Network. *Int J Recent Sci Res.* 8(12), pp. 22716-22720.
DOI: http://dx.doi.org/10.24327/ijrsr.2017.0812.1323

****