ISSN 2320-9984
Volume 4 Issue 4 | December 2016 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Study of Link Isolate for Trust Based Suspect On-Off Attack

Manisha Shrivastava
Research Scholar M. Tech.
Takshshila Institute of Engineering & Technology, Jabalpur (M.P.), [INDIA]
Email: mani.shrivastava.lbs@gmail.com

Abhishek Pandey
Assistant Professor
Takshshila Institute of Engineering & Technology, Jabalpur (M.P.), [INDIA]
Email: abhishekpandey@takshshila.org

***Abstract*—This is Review paper based on the study of Trust management for the on off attack . A trust management system is widely used for the decision making point of view in the different control policy. In this paper we are include the various kind of redemption scheme that used in Trust management system. In this paper we are include the basic information about the trust policy and malicious node that effect the management.**

Keywords:— *Trust management system, control policy, WSN, Malicious node*

1. INTRODUCTION

The decision making in a WSN is essential for carrying out certain tasks as it aids sensors establish collaborations. In order to assist this process, trust management systems could play a relevant role. In the context of a network, trust may help its elements to decide whether another member of the same network is being uncooperative or malicious. Hence, trust becomes quite important in self-configurable and autonomous systems, such as wireless sensor networks (WSN). The concept of trust[1] derives from sociological or psychological environments. Trust is an essential factor in any kind of network, social or computer networks. It becomes an important factor for members of the network to deal with uncertainty about the future actions of other participants. Thus, trust becomes especially important in distributed systems or internet transactions. As per the standard Definition [2] Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends Trust is a subjective phenomenon which is based on various factors or evidences. Reputation exists only in a community which is observing its members in one way or the other. Accordingly, reputation is the collected and processed information about one partner's former behavior as experienced by others. Based on [2-3], we try to give the following more detailed trust and reputation definition. Definition3. In a wireless network, a node S‟s trust in another node P is the subjective expectation of node S receiving positive outcomes through the transactions with node P. Definition 4. A node S‟s reputation is the global perception of its trustworthiness in the wireless network. Furthermore, the trustworthiness can be evaluated from its past and current behaviors.

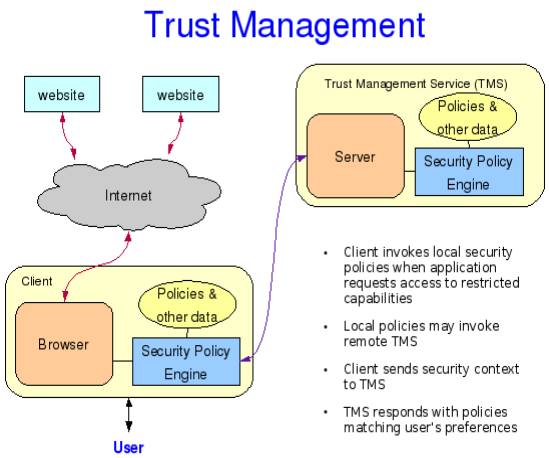

Figure 1: Trust Management

Trust management systems can be classified into two categories: credential-based trust management systems and behaviour-based trust management systems. This classification is based upon the approach used in order to establish trust among the peers of a system. Credential-Based Trust Management Systems- In this type of systems, peers (or nodes) use credential verification in order to establish trust with other peers (or nodes). The primary goal of credential-based trust management systems is to enable access control. Therefore their concept of trust management is limited to verifying credentials and restricting access to resources according to application- defined policies. A peer requests for access to a restricted resource. The access is controlled by a resource-owner that provides access only if it can verify the credentials of the requesting peer. Trust of the requesting peer in the resource-owner is not usually included. Thus, this type of systems is useful when there is an implicit trust in the resource-owner. However, these type of systems do not incorporate the need of the requesting peer to establish trust on the resource- owner. For this reason they are not very good trust management solutions for all decentralized systems. Examples of credential-based trust management systems are Policy Maker [9], its successor, Key Note [8] or Referee [10]. Behavior-Based Trust Management Systems- These types of systems are also called experience-based. In these models an entity trusts another entity based on past experience or behavior. Thus, entities can perform evaluation on the other entities based on these features. These systems are mainly based on the concept of reputation, which is quite related to the concept of trust. There have been many attempts to specify trust for different domains. Our interest focus on trust management for WSN. Very little has been done on this field, but some efforts have been carried out in quite related areas such as Ad-hoc and P2P networks. Most of the trust management systems developed for these kind of networks consist of collection of data and the application of a certain engine in order to compute that data. Most of these systems are based, or take into consideration, the concept of reputation. Once the reputation ratings of a system are collected, they should be computed. There exist different reputation engines. A classification of them can be found in [11].

2. TRUST MANAGEMENT SYSTEM IN DIFFERENT DOMAIN

Trust Management Systems for Ad Hoc Networks

In [10] the authors present a trust model for mobile Adhoc networks that can be used in a dynamic context within the routing process. Initially, each node is assigned a trust value according to its identity. For instance, if no information is available about the trustworthiness of a node the assigned value will be unknown. Each node records the trust levels about their neighbours. Then, by using simple, logical calculations similar to averages a node i can derive the trust level of node j, TLi (j). In [12] secure routing is also considered but the way of assigning the trust levels is carried out by evaluation of nodes over other nodes. Trust is evaluated considering factors such as statistics, data value, intrusion detection or personal reference to other nodes. The trust evaluation values, TE (i; j), are stored in a matrix. The final trust value is calculated via a linear function that uses the values stored in the matrix. Reputation is considered in [11] as a way for building trust. The mechanism builds trust through an entity called the trust manager. An important part of the trust manager is the reputation handling module. Each node monitors the activities of its neighbours and sends the information to the reputation manager. Then, the information is passed to the reputation handling moduleand the reputation values are obtained via simple metrics. Zhu et al [13] provide a practical approach to compute trust in wireless networks by viewing any individual mobile device as a node of a delegation graph G and mapping a delegation graph from the source node S to the target node T into an edge in the correspondent transitive closure of the

graph G, from which the trust value is computed.

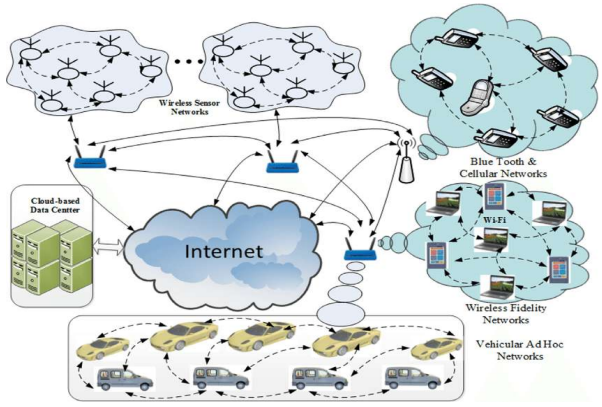

Figure-2-Architecture-of- ***Ad Hoc Networks***

Trust Management Systems for P2P Networks

PET [9] is a personalized trust model that evaluates risk and reputation separately in order to derive trust values. Reputation is also used as a way to obtain trust in [14]. In this work, when an agent wants to evaluate the trustworthiness of another agent, it starts to search for complaints on it. Once the data about the complaints is collected trust can be assessed by an algorithm proposed by the authors. Bayesian networks have also been used [3, 20]. Other approaches [18] use statistics methods such as standard deviation and mean in order to detect anomalies or malicious behaviour of peers. Trust Me [17] is a secure protocol for anonymous trust management that uses public-key cryptography. A similar approach is presented in [11] where the authors introduce a protocol based on a polling mechanism. This protocol also uses public key cryptography.

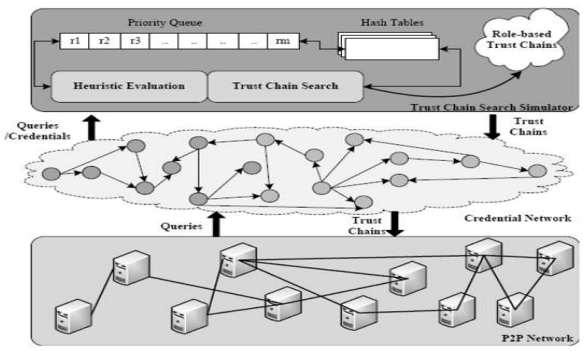

Figure 3: Heuristic Discovery of Role-Based Trust Chains in P2P Networks

Trust Redemption Scheme Because unintentional temporary errors may occur a redemption scheme is required to allow an untrusted node to recover its trust value. Redemption schemes can be classified in two ways. Behavior Based Redemption (BBR) recovers trust based on subsequent behaviors. Time Based Redemption (TBR) recovers trust periodically. If both BBR and TBR are used together, we refer to this as Combined Redemption. In the following sections, we classify existing trust models by these redemption schemes[4]. Behavior Based Redemption To understand Behavior Based Redemption, assume that a friend had a bad behavior in the past, but since then the friend has behaved very well several times. Thus, we can expect that the friend will behave well in the next behavior. Similarly in a distributed system, if a node behaves very well now, we can expect the node will behave well in the next behavior, even if the node had a bad behavior in the past. A representative scheme is presented in CORE [5]. CORE evaluates neighboring nodes based on direct observation, indirect observation that considers only positive reports by others, and task-specific behavior. These are compiled by a weighted trust technique, and the compiled result is used for discriminating and isolating a malicious node from the network. CORE assigns higher weight to past behaviors than recent behavior to minimize the influence of a recent bad behavior on the evaluation.

Time Based Redemption

If we assume that a friend had a bad behavior in the past, we might decide not to trust the friend for a while. After time has passed, we may expect the bad behavior was a mistake, and give the friend another chance. This represents Time Based Redemption. We provide some time to a node to recover from a temporary error, and we give another opportunity to behave well. For example, in [6] the authors propose OCEAN. In OCEAN negative behavior decreases the rating of the node more than positive behavior increments the rating. When the rating is below a

threshold, the node is added to the faulty list, and the faulty list is broadcast. Other nodes use this faulty list to avoid the malicious nodes.

Uncategorized Trust Management Schemes

There is many trust management schemes that do not employ any redemption at all. However, such trust management schemes could be combined with a redemption scheme such as those described above. For example, in the Micro-payment [7] scheme, a node receives one token for forwarding a message of another node, and such tokens are deducted from the sender (or the destination). The tokens are managed by one or more accounting center. This can be considered as a type of centralized trust management scheme since many tokens give more opportunities to be used, and fewer tokens might exclude the node from the system. Although the authors did not address redemption, if we consider the tokens to be Trust, this scheme could be classified as a BBR because good behaviors recover and bad behaviors decrease the number of tokens. In the Micro-payment scheme, we could also employ TBR by applying the concept of interest to the accounting center, and make it periodically increase the number of tokens.

3. CONCLUSION

In this paper we are include the basic introduction of TSM and TSM Redemption scheme. Here we are including the Trust Redemption Scheme and Time Based Redemption. This paper also includes the TSM in the some different domain**.**

REFERENCES:

[1] Sakshi Srivastava et al "A Survey on Reputation and Trust Management in Wireless Sensor Network" International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 1 Issue3 pp 139-149 August 2012 ISSN 2278 – 0882

[2] Josang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support System, Vol. 43, No. 2, 618-644. (2007).

[3] Gambetta, T.: Can we trust trust? In: D. Gambetta (Ed.), Trust: making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 213-238. (1990)

[4] Younghun Chae et al ." Trust Management for Defending On-Off Attacks" IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 4, April 2015 1045-9219_ 2014 IEEE. Personal use is permitted, but republication/ redistribution requires IEEE permission.

[5] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. IFIP TC6/ TC11 6th Joint Working Conf. Commun. Multimedia Security: Adv. Commun. Multimedia Security, 2002, pp. 107–121.

[6] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Technical report, Stanford University, NI/0307012, 2003

[7] M. Jakobsson, J.-P. Hubaux, and L. Butty_an, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," in Proc. Financial Cryptography, 2003, pp. 15 –33..

[8] M. Blaze, J. Feigenbaum, and A. D. Keromytis. Key Note: Trust Management for Public-Key Infrastructures (position paper). Lecture Notes in Computer Science, 1550:59{63, 1999.

[9] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In IEEE Symposium on

Security and Privacy, 1996

[10] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust Management for Web Applications. Computer Networks and ISDN Systems, 29:953{964, 1997

[11] A. Josang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, 2006

[12] Y. Rebahi, V. E. Mujica-V, and D. Sisalem. A Reputation-Based Trust Mechanism for Ad-hoc Networks. In 10th IEEE Symposium on Computers and Communications (ISCC 2005), 2005.

[13] Riaz Ahmed Shaik, Hassan Jameel, Sungyoung Lee, Saeed Rajput, and Young Jae Song. Trust Management Problem in Distributed Wireless Sensor Networks. In 12th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06), IEEE Computer Society, 2006

[14] J. Frey. Wisa Wireless Control in Theory, Practice and Production. Technical report, ABB, September 2008.