International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

DIFFERENT SECURITY THREATS IN SERVICE-ORIENTED AD HOC NETWORKS

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

M. Praveena,
Assistant Professor,
Department of Computer Science,
Dr.SNS Rajalakshmi College of Arts and Science,
Coimbatore, Tamilnadu, India.

Abstract: The service oriented ad hoc networks are consolidated with network service providers and service requestors. This kind of network doesn't like to have malicious nodes which may collude to maximize their own gain and even monopoly service. Trust calculation for finding malicious service requestor as well as service providers are much complicated. The trust management suffers from several attacks and issues such as bad mouthing attack, self promotion, ballot stuffing and opportunistic service attacks etc., This paper provides the survey of various techniques and methods involved with the trust calculation and multi objective optimization in service oriented ad hoc networks.

Keywords: Mobile Ad hoc network, Trust Management, Security, Task assignment, Service Discovery.

I.INTRODUCTION

Ad-hoc networks are the decentralized type of wireless networks that work without the help of a centralized control and with the features such as openness, distributed communication, self-configuration, self-organization, and limited bandwidth wireless channels [1]. These networks are composed of tiny and low-cost sensing and communication devices with the features such as limited communication range, processing speed, memory, and battery energy. Due to the limited communication range, nodes follow multi-hop routing to transmit the information between the source and destination nodes. In this process, nodes act as the router to identify the path, and as the host to generate the data and control packets. Therefore, in ad-hoc networks, node cooperation is a vital factor for executing the protocol instructions. Due to the openness and infrastructure-less network operations, Mobile ad-hoc networks (MANETs) have gained significant attention in performing mission critical tasks in remote and hostile environments. However, the limitations of these networks such as utilization of insecure wireless channels, remote deployment, distributed communication; self-organization, self-configuration, and utilization of limited bandwidth wireless channels introduce several security vulnerabilities. Further, nodes are subject to physical capture and tamper by an adversary due to lack of tamper proof bodies. An adversary may extract the information of nodes such as identity, location data, and secret key material. These tampered nodes may be kept back in the network to gain control over the network activities. These compromised nodes may exhibit malevolent behavior and thwart the network operations by launching various security attacks. The behavior of a compromised node can be either selfish or malicious. Selfish behavior node does not harm the network operations; however, it does not cooperate in the network operations due to the resource limitations (such as low battery energy or to preserve bandwidth). On the other hand, malicious behavior is an active attack in which the compromised nodes intentionally harm the network operations. So in order to reduce the damages of data and connections on the wireless network, the trust calculation is created. Service selection and task assignment are performed using the trust evaluation [2]. In this paper, we surveyed various techniques and methods involved in the trust-based service selection and solutions against various security attacks. In a service-oriented MANET, there are several objectives to be considered. The initial objective is maximizing mission reliability based on task completion proportion; the next objective is to minimize utilization variance, leading to high load balance among all nodes and to minimize the delay to complete time-sensitive tasks, thus maximizing the quality of service (QoS).

A. Trust in MANET:

Trust in MANET is the analysis of node in terms of "firm faith in the reliability, truth, or ability of someone or something". It is the degree of belief about the behavior of a particular node. In MANETs, due to high mobility, malicious nodes may frequently join and leave the network. At this point, nodes have to trust each other to initiate the information exchange. Trust is a dynamic one, which is not same always. The positive behavior can increase the trust and negative case decreases. As a result, trust values vary over time. Trust in MANET is asymmetric that two nodes may not have same trust in each other. And this is a context dependent process in nature. It means the degree of trust will be based on context and application involved. The trust value is influenced by a mobile node and its observation of behavior on other nodes.

Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. Trust reflects expectations on the honesty, integrity, ability, availability and quality of service. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted. In MANETs, an untrustworthy node can cause considerable damage and adversely affect the quality and reliability of data. The trust computations classification is as shown in Figure 1.0.

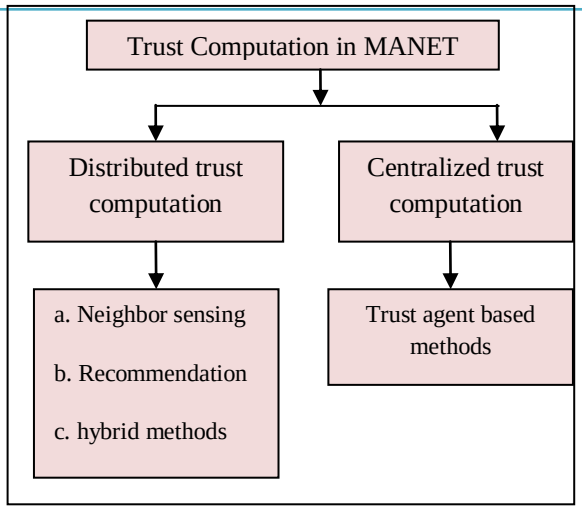

Figure 1.0 trust computation methods

In Distributed Trust Computations every node computes its own value of trust on its neighbors and it can be classified as direct trust, indirect trust and hybrid. Based on the type different approaches and techniques have been applied.

Neighbor Sensing (Direct Trust): Distributed trust computation based on neighbor sensing, where every node observe neighbors for their event reports and store the reports in 'knowledge' cache.

Recommendation Based Trust: Distributed trust computations based on recommendation systems. Here, trust relationships on nodes are established based on recommendations alone.

Hybrid Method: In this method the trust on a node is computed based on direct experience and also recommendations from other nodes.

The trust agent based methods under centralized trust computation techniques are depends on the third party server or node to evaluate the trust score of others. The centralized approach may not perform well always. So the selection and computation of trust scores are based on the network size and other resource details.

II.LITERATURE REVIEW

A service-oriented MANET is affected by numerous malicious behaviors such as Bad-mouthing attacks, opportunistic service attack, ballot-stuffing attack etc., at the time of trust calculation the behavior of every node or service provider should carefully validated.

Bad-mouthing attacks:

In the service oriented MANET, bad mouthing attacks are the fake feedbacks about a node by a malicious node to spoil the reputation of the particular node in the network.

The badmouth attackers deliberately disseminate false trust values to lower the reputation of a well-behaving node. Therefore, nodes have to validate the trust values before going to use them with the direct trust values. Furthermore, the trust propagation in the literature is modeled as proactive or on-demand. In the paper [3], nodes periodically disseminate the neighbor based trust value calculation via special control packets. In the latter approaches [4][5], nodes obtain neighbor trust values only when they are required. However, in all approaches, the trust values have to be disseminated using special control packets and hence it may increase the communication overhead. To this end, in the current work, a special technique is used to reduce the communication overhead.

In the paper [6], detection of bad mouthing attacks and trust calculation is performed using SOM (self-Organizing Maps). The authors have proven that the SOM is capable of attaining 100% detection rate with 0% false positive rate. This is only possible when it is trained with clean. At last, when 28.6% of the nodes are malicious, the detection of the attack is possible if at least 40% of the data are clean.

The majority of the previous solutions in the literature for handle bad-mouthing attack rely on prevention techniques. A distinctive approach is presented in the paper [7], which relies on cryptography protocols. But, with the existence of side channel attacks [8], the attacker can easily guess the secret keys and compromise the cryptography based protocols. One more approach proposed with controlled anonymity [9], where the identities of the communicating entities are not known to each other. In this way, each entity has to provide ratings based on the quality of service provided, and as they can no longer identify their "victims", bad-mouthing and negative discrimination can be avoided. Still, this is not always possible and it will not protect the system from all the attacks. Thus, a second line of defense that would detect the attacks and stop their further spreading is necessary.

***Ballot-stuffing attacks*:** in this type of attack, a malicious node may collude with other malicious nodes to boost the reputation of a bad node by providing good and positive recommendations for the bad node. Using this way, it will try to increase the chance of the bad node being selected for task execution. There are only few researches concentrated on this attack, the trust protocol in [10] deals with ballot-stuffing attacks also by belief discounting. Very few authors proposed techniques to handle ballot-stuffing attacks on hardware applications such as electronic voting machine etc., however, there is no specific application yet to be implemented in MANET.

***Opportunistic service attacks*:** Every trust calculation is based on the reputation score, so every malicious node will provide high-quality service to obtain high reputation score at the time of low trusted scenario. And the same node will provide worst service when the reputation score is high. In paper [11], authors designed a protocol for effective spectrum sharing by accurately detecting non-jamming and DOS attacks. Using such protocol, opportunistic service and other service oriented attacks are eliminated. The trust protocol in [10] also deals with opportunistic service attacks by severely punishing nodes that fail to provide the advertised service quality during task execution.

Following the Byzantine Failure model [11], we assume that a task fails when at least 1/3 nodes providing bad service. Here we note that with good reputation, a malicious node can effectively collude with other bad nodes to perform bad-mouthing and ballot-stuffing attacks. Hence, a malicious node will provide good service at its true service capability most of the time in order to gain high reputation. However, a malicious node can opportunistically collude with other

malicious nodes to fail a task, when it senses that there are enough bad nodes around (at least 1/3) at the expense of trust loss.

Self-promotion attacks: A malicious node can boost its service quality or lie about its utilization information so as to increase its chance of being selected as the SP. the trust protocol in the literature deals with self-promotion attacks by severely punishing nodes that lie about their utilization or fail to provide the advertised service quality during task execution. In practice, self-promotion attacks can be easily detected, and as a result a malicious node would expose itself as vulnerable, resulting in a low reputation. This attack is less likely to be performed by a smart attacker.

Recently, authors in [12] proposed a mechanism to eliminate the recommended trusts when it is given by the low trustworthy nodes. The algorithm used a mechanism to filter out the recommended trusts shared by low trustworthy nodes along with high deviated trusts shared by trustworthy nodes. The mechanism is based on two different assumptions one is, Recommendations shared by a low trustworthy node will be considered as dishonest recommendation and another one is Recommendation shared by a trustworthy node but is far away from the mean trust value will be considered as dishonest recommendation.

Conflicting behavior attacks: in this type of attack, a malicious node can selectively provide adequate, appropriate response and service within its capability for some service requestors. At the same time the node may not provide satisfactory service for other nodes. This type of behavior is usually called as selfish attack; it assumes that malicious nodes know each other; therefore with conflicting behavior attacks a malicious node will provide satisfactory service to other malicious nodes, but unsatisfactory service to trust worthy and legitimate nodes.

Random attacks: At the time of conflicting behavior by a service provider or other node, a malicious node can perform random attacks by providing unsatisfactory service to legitimate and trustworthy nodes. And this will be performed erratically, so as to avoid being labeled as a low service trust node and risk itself not being selected as a SP by non-malicious SRs in the future. In the random attacks, a malicious node will provide bad services on random nodes and requests, so as not to risk it being labeled as a node providing bad service and not being selected for service. With opportunistic service attacks, a malicious node may not perform persistent attacks all the time but rather can attack opportunistically. In order to manage the opportunistic service attacks in service oriented MANET, the condition under which an opportunistic service attack or a time varying attack will perform may be represented as a context service quality relationship for trust calculation to learn dynamically [13].

Paper ID	Technique	Attack type	Advantages	disadvantages
6	SOM	Bad-mouthing attack	Detection rate is high and 0% false positive rate. So accuracy is high.	Ned more trained and clean dataset to find the attacks.
7,8	Cryptography based protocols	Bad-mouthing attack	Protects the data using cryptographic	Not secure and failed to detect bad-mouthing attack completely. It can be affected by the side channel attacks
9	Controlled anonymity	Bad-mouthing attack	negative discrimination can be avoided	Not possible and valid always.
10	Trust protocol	Ballot-stuffing attacks/ Opportunistic service attacks	Find attacks with trust scores	Not cost effective.
11	Trust spectrum sharing	Opportunistic service attacks	Data and service losses arise.	Failed to find conflict behaviors
12	trust-based heuristic algorithm	All types of attacks	Useful for dynamic trust protocol management to maximize application performance in terms of MOO.	Not suitable for anonymous networks
13	CATrust	Ballot-stuffing attacks/ ***Random attacks/*** Opportunistic service attacks	Handles uncertainty in detection	Concern on social behavior can lead the solution best.
14	PSO(particle swarm optimization technique)	Service oriented attacks	Effective for cloud environment	Ned higher training samples
15	energy-efficient task assignment protocol	None	Effective task allocation for sensor network	Not suitable for MOO problem
16	trust-based solution for task assignment	Service oriented attack	Suitable for grid management	Computation overhead is high.

Table 1.0 comparative table

The table 1.0 shows the comparative analysis of different techniques and methods for trust calculation in service oriented MANET. Continuously, we perform a comparative analysis of different protocols of MANET which provides trust management. The protocols such as CATrust, STO, and trust-based heuristic algorithm as the underlying trust protocol for the trust-based algorithm for solving the service composition and binding MOO (Multi objective optimization) problem.

Author Guo et al. [14] examined a task assignment problem using a particle swarm optimization (PSO) technique that minimizes task execution time and cost for data transfer between processors in cloud computing environments. However, the PSO process needs a huge cost to deploy.

Xie and Qin [15] proposed an energy-efficient task assignment protocol based on the tradeoff between energy and delay to execute a task for collaborative networked embedded systems to minimize the length of schedules of task allocation and energy consumption.

Author Shen et al. in [16] developed a trust-based solution for task assignment in grid management with multiple system objectives including security, reliability, load balance, and throughput. This solution is much reliable because it concentrated on more properties. However, all the methods are not completely identified the selfish and other service oriented attacks. Solutions fall under trust management assume no malicious entity in the system, which is not a valid assumption in a service-oriented MANET environment which very likely will be populated with malicious nodes acting for own interest and colluding for individual welfare.

III.PROBLEM DEFINITION

From the analysis, there are few major problems of existing solutions are found. The existing algorithms and methods does not considering the existence of malicious nodes acting for their own interest and colluding for individual welfare, which is stated in the list of attack and solving the task assignment MOO problem in exponential time complexity, making it unsuitable for runtime deployment. In [12], authors developed a trust-based solution to overcome the different types of attacks and problems. In particular, the authors developed a trust-based algorithm to solve the task assignment MOO problem. Along with the certain algorithms, the set of security threats have been handled.

IV.CONCLUSION

Despite of advantages, existing trust models suffer from following limitations. Most of the models cannot detect multiple security attacks on data aggregation such as bad mouth attack, ballot-stuffing attack, service oriented attacks, dynamic attacks and selfish attacks, and energy based attacks. These trust models do not prevent the possibility of malicious or selfish node to be selected as CH. This may influence the network performance such as packet delivery. Trust metrics used by the methods are insufficient for dynamic detection and isolation of malicious nodes. Since the nodes are densely deployed in the MANET, lightweight reputation and trust score exchange is required to reduce communication overhead. Systematic evaluation of direct and indirect trust values is required to enhance the network lifetime. Along with the trust model, utilization of the trust management and service allocation may improve the detection accuracy of the malicious nodes in the network. Since using MOO reputation and trust calculation at node level may drain the node energy faster, its advantage can be utilized fully by implementing it at the selected node. With this observation and the aforementioned limitations the further work will be defined.

V.REFERENCES

[1] Giordano, Silvia. "Mobile ad hoc networks." *Handbook of wireless networks and mobile computing* (2002): 325-346.

[2] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "A survey on trust management for mobile ad hoc networks." *IEEE Communications Surveys & Tutorials* 13.4 (2011): 562-583.

[3] Li, Xiaoqi, Michael R. Lyu, and Jiangchuan Liu. "A trust model based routing protocol for secure ad hoc networks." *Aerospace Conference, 2004. Proceedings. 2004 IEEE*. Vol. 2. IEEE, 2004.

[4] Virendra, Mohit, et al. "Quantifying trust in mobile ad-hoc networks." *Integration of Knowledge Intensive Multi-Agent Systems, 2005. International Conference on*. IEEE, 2005.

[5] Liu, Zhaoyu, Anthony W. Joy, and Robert A. Thompson. "A dynamic trust model for mobile ad hoc networks." *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*. IEEE, 2004.

[6] Banković, Z., et al. "Detecting bad-mouthing attacks on reputation systems using self-organizing maps." *Computational Intelligence in Security for Information Systems*. Springer Berlin Heidelberg, 2011. 9-16.

[7] Jing-Kai Lou, Kuan-Ta Chen, and Chin-Laung Lei. A collusion-resistant automation scheme for social moderation systems. In 6th IEEE Conference on Consumer Communications and Networking Conference, pp. 571-575. IEEE Press, Piscataway, NJ, USA (2009)

[8] Bar El, H. Introduction to Side Channel Attacks. White Paper, Discretix Technologies Ltd., (2003)

[9] Dellarocas, C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In 2 nd ACM conference on Electronic commerce, pp. 150--157. ACM, New York, NY, USA (2000)

[10] Wang, Yating, et al. "Trust-Based Task Assignment With Multiobjective Optimization in Service-Oriented Ad Hoc Networks." *IEEE Transactions on Network and Service Management* 14.1 (2017): 217-232.

[11] Jakimoski, G., and K. P. Subbalakshmi. "Denial-of-service attacks on dynamic spectrum access networks." *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*. IEEE, 2008.

[12] Islam, M. Hasan, and Adnan Ahmed Khan. "Detection of dishonest trust recommendations in

mobile ad hoc networks." *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*. IEEE, 2014.

[13] Wang, Yating. "Trust-Based Service Management for Service-Oriented Mobile Ad Hoc Networks and Its Application to Service Composition and Task Assignment with Multi-Objective Optimization Goals." (2016).

[14] L. Guo, G. Shao, and S. Zhao, "Multi-Objective Task Assignment in Cloud Computing by Particle Swarm Optimization," in *8th Int. Conf. Wireless Communications, Networking and Mobile Computing*, 2012, pp. 1- 4.

[15] T. Xie and X. Qin, "An Energy-Delay Tunable Task Allocation Strategy for Collaborative Applications in Network Embedded Systems," IEEE Trans. Comput. , vol. 57, no. 3, 2008, pp. 329-343.

[16] L. Shen, L. Zhang, and D. Huang, "Trust-Driven Both-Matched Algorithm for Grid Task Multi-Objective Scheduling," in *2nd Int. Conf. Information Science and Engineering*, 2010, pp. 1661–1664.

