International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Trust Management Schemes for Secure Data Transfer in MANETs : A Survey

N. D. Sukirtha Priya, T. Parameswaran

Department of Computer Science and Engineering, Anna University Regional Campus, Coimbatore, Tamil Nadu, India

ABSTRACT

Mobile Ad hoc Network (MANET) is an autonomous collection of mobile devices (sensors, smart phones, laptops, etc.) that connect with each other over wireless links and collaborate in a scattered manner to provide the required network functionality in the nonexistence of a fixed infrastructure. Trust Management in MANET is challenging when collaboration or cooperation is critical to accomplishing a task and system goals such as availability, reliability, scalability, and reconfigurability. In this paper, we have provided a survey of various schemes developed for trust management in MANETs.

Keywords : Trust, Trust Management, Mobile Ad Hoc Networks.

I. INTRODUCTION

A mobile ad hoc network [1] comprises of wireless mobile nodes forming a temporary network where nodes communicate through multi-hop without the help of centralized infrastructure. There are various technical challenges in security protocol design due to severe resource constraints in bandwidth, memory size, computational power, battery life, and unique wireless characteristics such as , lack of specific ingress and exit points, openness to eavesdropping, high security threats, vulnerability, untrustworthy communication, and advancement in topologies or memberships because of user mobility or node failure [2].

II. METHODS AND MATERIAL

1. Motivation for Trust Management in MANETS

The term, Trust Management, recognized as a distinct component of security services in networks and clarified that ”Trust management provides a unified approach to specify and interpret security policies, credentials, and relationships.”[3]. Trust management is needed when participating nodes desire to establish a network with an acceptable level of trust relationships among themselves. The elements across the communications network are the information transmitted, the sources of information, the processors of information, etc., should be taken into account of trust in MANETs. This trust must repeatedly be resultant under time-critical conditions, and in a distributed way.

Also, trust management has diverse applicability in many decision-making situations which include intrusion detection, access control, authentication, key management, isolating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in MANETs is also much more challenging than in traditional centralized environments.

The properties of trust in MANETs are: Trust is dynamic, subjective, context-dependent, asymmetric, and not necessarily transitive and reciprocal. Attacks considered in existing trust management systems in MANETs are Routing loop attacks, Wormhole attacks, Blackhole attacks, Grayhole attacks, DoS attacks, False information or false recommendation, Incomplete information, Packet modification/insertion, Newcomer attacks, Sybil attacks, Blackmailing, Replay attack, Selective misbehaving attacks, On-off attacks, and Conflicting behavior attacks.

Metrics considered by MANET trust management systems include overhead, throughput, goodput, packet dropping rate, delay, and route usage [2].

Cho et. al [2] described various trust management schemes based on specific design purposes such as authentication, secure routing, intrusion detection, access control (authorization), and key management. Also summarized 45 trust management schemes proposed for MANETs during 2000-2009 based on their design purposes. Despite a couple of surveys in trust management, a comprehensive survey of trust management in MANETs does not exist after 2009 and is the main aim of this paper. In this paper, we have summarized the schemes proposed after 2009.

2. MANET TRUST MANAGEMENT SCHEMES

This section summarizes trust management schemes that were developed for MANETs.

2.1 Routing Protocol Based Shared and Session Key Exchange Protocol

In this key exchange protocol, an algorithm was proposed to exchange shared and session key between the sender and destination during the route creation. This protocol has very less overhead since the key can be shared during regular route discovery. Shared key encryption is simple and fast which would make MANET data exchange faster. If the key is suspected to be compromised, a new key can be discovered. No intermediate node can forecast the key unless most of the intermediate nodes are impaired. The main weakness of the protocol is that if the number of paths is small and one or more nodes are common to all the paths then that particular node(s) can calculate the key. However, the receiving node can determine such circumstance and discard such key and generate a new one. Moreover, if the nodes have mobility, they can change their geographical location to make the key stronger [4].

2.2 Scalable Maturity-Based Model

This model builds a trust relationship between nodes in the ad-hoc network. The trust is based on previous individual experiences and the recommendations of others. Recommendation Exchange Protocol (REP) is presented in which nodes are allowed to exchange recommendations about their neighbors. It does not require disseminating the trust information over the entire network. Rather, nodes only need to retain and swap trust information about nodes within the radio range. It relieved the effect of colluding attacks composed of liars in the network [5].

3.3 cTrust

In a cyclic mobile ad hoc network (cMANET), nodes move periodically. Unlike trust management in conventional schemes, not only neighbor trust relationships but also location and time factors are also involved in Trust management in cMANET. The cTrust scheme, a decentralized and self-configurable trust aggregation scheme, is proposed to handle trust establishment and aggregation issues. Trust relations are modeled as a trust graph in cMANET to enhance accuracy and efficiency of trust establishment among nodes. With increasing scale of ad hoc networks and complexities of trust topologies, cTrust scales well with marginal overheads [6].

3.4 Reputation-Based Trust Management System

Reputation-based trust management system was proposed for detecting and preventing MANET vulnerabilities. This scheme helps the nodes to exclude both active (malicious nodes) and passive (selfish nodes) attacks from the network while tolerating transient faults. The method work with any on-demand routing protocol [7].

3.5 Trust Management Model

This scheme allows nodes to evaluate the trust by taking into account certificate of other nodes to overcome vulnerabilities. The transmission over the shared wireless channel is in the order of milliseconds for different traffic conditions in wireless ad hoc networks as the time taken by the scheme is significantly less[8].

3.6 Trust-Based Routing and Intrusion Detection

A highly scalable cluster-based hierarchical trust management protocol is proposed to deal with selfish or malicious nodes effectively. Multidimensional trust attributes derived from communication and social networks are considered to evaluate the overall trust of a sensor node. It is found that trust-based geographic

routing approaches the optimal performance level attainable by flooding-based routing in message delivery ratio and message delay without incurring substantial message outlay. For trust-based intrusion detection, it is discovered that there exists an ideal trust threshold for minimizing false positives and false negatives and trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability [9].

3.7 Iterative Algorithm for Trust Management and Adversary Detection

Delay/Disruption Tolerant Networks (DTNs) were identified as one of the main areas in the field of wireless communication, wherein sparseness and delay are unusually high. Using reputation-based trust management system in MANETs is shown to be an effective way to handle the adversarial nature in Mobile Ad hoc Networks (MANETs). Nonetheless, because of the unique characteristics of DTNs, those traditional techniques do not apply to DTNs. A repeated malicious node detection mechanism for DTNs referred as ITRM is developed. This scheme is a graph-based iterative algorithm inspired by the success of previous message passing methods for decoding low-density parity-check codes over bipartite graphs. Employing ITRM to DTNs for several mobility models, it is observed that this iterative reputation management scheme is effective than other well-known reputation management techniques such as the Eigen Trust and Bayesian framework. Further, it provides high data availability and packet-delivery ratio with low latency under various adversary attacks [10].

3.8 Integrated Social and Quality of Service Trust Management

Social trust derived from social networks and quality-of-service (QoS) trust derived from communication networks are combined to attain a composite trust metric as a base for evaluating trust of mobile nodes. The peer-to-peer subjective trust as a result of executing distributed trust management protocol is close to ground truth condition over an extensive range of operational and environment conditions with high resiliency to malicious attacks and misbehaving nodes [11].

3.9 Trust-enhanced anonymous on-demand routing protocol (TEAP): TEAP is proposed for restraining the exploitation of anonymity in two ways. In the first method, if any cooperative message is not sent upon receiving two warnings then the user is exposed as a trespassing user to other users. In the second method, if a user tries to send multiple claims across a specific user for the same reason it will also be treated as a trespassing user. The TEAP protocol design is based upon broadcast with trapdoor information which is used to detect the misbehaving users anonymously in the network [12].

3.10 Reliable and secure source routing

Enhanced reliability and security is achieved by the maintenance of a reliability factor by the nodes, which is increased when nodes participate successfully in data transmissions. This is determined through the use of positive and passive acknowledgments. Additional optimizations are included to increase the efficiency and performance of the network [13].

3.11 Distributed Cooperative Trust Based Intrusion Detection Framework

An intrusion detection architecture is introduced based on trust relationship and cooperation. It awaits on local and global determination of attacks within network and intrusion detection is carried out in a distributed fashion. Reputation mechanism is used for trust assessment, which is obtained by watching the neighbor nodes behaviors. IDS alert messages are used to disseminate evidence of an intrusion attempt. A distributed IDS engine is the focal point of the architecture and aimed to utilize a cooperative trust based intrusion detection system to cope with the disadvantages drawn from mobility of nodes [14]

3.12 Recommendation Based Trust Model

With an Effective Defence Scheme Recommendation based trust management was proposed to filter out the misbehaving nodes while searching for a packet delivery route. A recommendation based trust model with a defense scheme utilizes clustering technique to dynamically filter out attacks related to dishonest recommendations between the certain time, based on many interactions, compatibility of information and closeness between the nodes [15].

3.13 Unified trust management scheme using unsure Reasoning

Using recent advances in uncertain reasoning originated from the artificial intelligence community, a unified trust management scheme was proposed to enhance the security. In this scheme, the trust model has two components: trust from direct observation and trust from indirect observation. In direct observation, the trust value is derived using a type of uncertain reasoning called Bayesian inference, when the adequate probability model can be characterized. On the other hand, with indirect observation, the trust value is derived using another type of uncertain reasoning called Dempster-Shafer theory, when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, more exact trust values of the observed nodes can be acquired. Throughput and Packet delivery ratio is improved significantly with slightly increased average end-to-end delay and overhead of messages [16].

3.14 Two-Dimensional Trust Levels

Two dimensions of trust levels are utilized and evaluated by either a trusted server or individual PSN nodes or both to control PSN data access in a heterogeneous manner by attribute-based encryption. Extensive analysis and performance evaluation based on implementation showed that this scheme is highly efficient and provably secure under the relevant system and security models [17].

3.15 Trust based Information Sharing Model (TRUISM)

In this recent multi-hop recommendation based trust management scheme, Dempster-Shafer theory is modified that can efficiently combine recommendations from multiple devices in the presence of unpredictable and malicious recommendations. A recommendation-routing protocol named 'buffering on-the-fly' was introduced to reduce the number of recommendation traffic by storing trust values in intermediate nodes. Trust based Information Sharing Model afford a flexible behavioral model for trust estimation where a node can prioritize recommendations based on its requirements. It performed well in the presence of contradictory recommendations, also ensures a faster and scalable trust-based information sharing by reducing the overall packet flow in the system [18].

3.16 Bias minimization and application performance maximization

This scheme addressed the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization. Identified and validated the best trust protocol settings under which trust bias is minimized, and application performance is maximized. The effectiveness of this approach is demonstrated with an integrated social and quality-of-service (QoS) trust protocol (called SQTrust) with which the best trust aggregation setting is identified under which trust bias is minimized despite the presence of malicious nodes performing slandering attacks. Furthermore, using a mission-oriented mobile group utilizing SQTrust, the best trust formation protocol setting identified under which the application performance regarding the system reliability of the mission-oriented mobile group is maximized [19].

3.17 Probabilistic Misbehavior Detection Scheme iTrust

Probabilistic misbehavior detection scheme was proposed for secure DTN routing toward efficient trust establishment. iTrust introduced an idea that a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidence and probabilistically checking. iTrust was modeled as an inspection game. "It uses game conjectural inquiry to operate that by fixing an appropriate investigation probability, TA could assure the security of DTN routing at a minimum cost". To improve the efficiency of the scheme, detection probability is correlated with a node's reputation, which allows a dynamic detection probability determined by the trust of the users [20].

3.18 Trust Evaluating model

A new trust evaluation model proposed to quantify the trust level of the nodes in MANETs. This trust evaluation model introduced a new evaluation function for computing direct trust value and a new relationship function to merge the direct trust and other's recommendation. It dealt with the fundamental trust

establishment problem and served as the building block for higher level security solutions [21].

3.19 Trust based routing mechanism

The optimized link state routing (OLSR) protocol is an efficient, proactive routing protocol which is very suitable for such dense and large-scale MANET. However, in both data plane and routing plane, OLSR-based MANET suffers from many serious security threats which are difficult to resist via traditional security mechanisms. In this trust-based routing mechanism, a trust reasoning model based on fuzzy Petri net is presented to evaluate trust values of mobile nodes. Also, to avoid malicious or compromised nodes, a trust-based routing algorithm is proposed to select a path with the maximum path trust value amidst all possible paths. OLSR is enhanced by using the trust model and trust-based routing algorithm, called FPNT-OLSR. The trust factor collecting method is an efficient trust information propagating method, which does not generate extra control messages. FPNT-OLSR is very effective in establishing secure routes. It also performed better than existing trust-based OLSR protocols regarding packet delivery ratio, average latency and overhead [22].

3.20 T2AR: Trust-aware ad hoc routing protocol

A trust-aware ad-hoc routing (T2AR) protocol is proposed to improve the trust level between the nodes. This method modifies the conventional AODV routing protocol with the constraints of energy, trust rate, mobility based malicious behavior prediction. The packet sequence ID matching from the log reports of neighbor nodes calculate the trust rate that avoids the malicious report generation. Also, the direct and indirect trust observation schemes utilization increases the trust level. The received signal strength indicator utilization determines the trusted node be within the communication range or not. The comparative analysis between the T2AR with the existing methods such as TRUNCMAN, RBT, GR, FBR and DICOTIDS regarding the average end-to-end delay, throughput, false positives, packet delivery ratio shows the effectiveness of T2AR [23].

3.21 Threshold based Public Key Management

This is a fully distributed trust-based public key management approach utilizing a soft security technique based on the trust concept. Instead of using hard security approaches to eliminate security vulnerabilities, this work aimed to maximize performance by relaxing security necessities based on the perceived trust. A composite trust-based public key management (CTPKM) is proposed with the goal of maximizing performance while alleviating security vulnerability. Every node applies a trust threshold to determine whether or not to trust another node. An optimal trust threshold exists to meet the convicting goals between performance and security, by exploiting the inherent trade-off between trust and risk. The CTPKM minimizes risk (i.e., information leak out) using an optimal trust threshold while maximizing service availability with acceptable communication overhead incurred by trust and key management operations. CTPKM outperforms both existing non-trust-based and trust-based counterparts [24].

3.22 Location-Based On-Demand Routing on Privacy-Preserving

A location-based on-demand anonymous MANET routing protocol is timbered that accomplish privacy and security against both outsider and insider adversaries [25].

III. RESULTS AND DISCUSSION

Arduino is a compu

IV.CONCLUSION

In this paper, we have discussed an introduction to trust management, the motivation for trust management, attacks considered in existing trust management systems, an understanding of trust properties that are observed in developing trust metrics for evaluating trust in MANETs. Further, we surveyed and summarized various trust management schemes in MANETs.

V. REFERENCES

[1]. Antesar M. Shabut, Keshav P. Dahal, Sanat K. Bista, Irfan U. Awan "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs" IEEE Transactions On Mobile Computing, Manuscript Id 2013

[2]. Arijita Banerjee Sarmistha Neogy Chandreyee Chowdhury "Reputation Based Trust Management System for MANET" 2012 Third International Conference on Emerging Applications of Information Technology (EAIT) (IEEE)

[3]. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proc. IEEE Symposium on Security and Privacy, 6-8 May, 1996, pp. 164 - 173.

[4]. Brijesh Kumar Chaurasia1,* and Ranjeet Singh Tomar2"Trust Management Model for Wireless Ad Hoc Networks Proceedings" of the International Conference on SocProS 2011, AISC 130, pp. 201–206. Springer India 2012

[5]. J. H. Cho, A. Swami and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," in IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011.

[6]. S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[7]. Erman Ayday, and Faramarz Fekri,"An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks ", IEEE IEEE Transactions On Mobile Computing, Vol. 11, No. 9, September 2012

[8]. Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" By Ieee Transactions On Network And Service Management, Vol. 9, No. 2, June 2012

[9]. M.D. Golam Kaosar,"Routing Protocol Based Shared and Session Key Exchange Protocol for Wireless Mobile Ad-hoc Network"

[10]. Gayathri Dhananjayan and Janakiraman Subbiah SpringerPlus " T2AR: trust aware ad hoc routing protocol for MANET ", 2016 Elsevier

[11]. Haojin Zhu, , Suguo Du, Zhaoyu Gao, Mianxiong Dong, Member, IEEE, and Zhenfu Cao,"A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014

[12]. Huanyu Zhao, Xin Yang and Xiaolin Li "cTrust: Trust Management in Cyclic Mobile Ad Hoc Networks", Member, IEEE 2011 IEEE

[13]. Ing-Ray Chen, Jia Guo, Fenye Bao "Integrated Social and Quality of Service Trust Management of Mobile Groups in Ad Hoc Networks" 2013 – IEEE

[14]. Ing Ray Chen a,⇑, Jia Guo a, Fenye Bao a, Jin-Hee Cho "Trust management in mobile ad hoc networks for bias minimization and application performance maximization ",2014 Elsevier B.V.

[15]. Imad Jawhar • Zouheir Trabelsi • Jameela Al-Jaroodi "Towards more reliable and secure source routing in mobile ad hoc and sensor networks" © Springer Science+Business Media New York 2013

[16]. Jin-Hee Choa,_, Ing-Ray Chenb, Kevin S. Chana Elsevier "Trust Threshold based Public Key Management in Mobile Ad Hoc Networks" Volume 44, 1 July 2016, Pages 58–75

[17]. Karim El Defrawy, Member, and Gene Tsudik,"Privacy-Preserving Location-Based On-Demand Routing in MANETs" Journal On Selected Areas In Communications, Vol. 29, No. 10, December

[18]. Khalid Zaman Bijon_, Md Munirul Haquey and Ragib Hasany "A TRUst based Information Sharing Model (TRUISM) in MANET in the Presence of Uncertainty" By 2014 Twelfth Annual Conference on Privacy, Security and Trust (PST) (IEEE)

[19]. Muthumanickam Gunasekaran1, Kandhasamy Premalatha "TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks The Institution of Engineering and Technology (IET) Information Security.", 2013, Vol. 7, Iss. 3, pp. 203–211

[20]. Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity- Based Model" IEEE Transactions On Network And

Service Management, Vol. 7, No. 3, September 2010

[21]. Shuaishuai Tan a, Xiaoping Li a, Qingkuan Dong ”Trust based routing mechanism for securing OSLR-based MANET”, 2015 Elsevier B.V.

[22]. Sureyya Mutlu “Simulation And Performance Analysis Of Distributed Cooperative Trust Based Intrusion Detection Framework For MANETs” Received: 03rd April 2013, Accepted: 03rd July 2013 Journal Of Aeronautics And Space Technologies July 2013 Volume 6 Number 2 (49-57)

[23]. Xia Li1, Jill Slay 1, Shaokai Yu “Evaluating Trust in Mobile Ad Hoc Networks ResearchGate” 07 February 2014. (Article)

[24]. Zheng Yan, and Mingjun Wang “Protect Pervasive Social Networking Based on Two-Dimensional Trust Levels” IEEE SYSTEMS JOURNAL 2014

[25]. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason “Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning” IEEE Transactions on Vehicular Technology 2013