http://dx.doi.org/10.21172/ijiet.81.041

Double Face Attack Resistant Trust Management Frameworks in Mobile Ad Hoc Networks: A Survey

Vaishali V. Sarbhukan
Department of Computer Engg.
Bharati Vidyapeeth College of Engg., Sec 4 CBD Belpada,
Navi Mumbai, Maharashtra , India

Dr. Lata Ragha
Department of Computer Engg.
Fr. C. Rodrigues Institute of Technology, Vashi
Navi Mumbai, Maharashtra, India

Abstract—Trust management is a promising approach to conduct node's transactions and establish management interactions in distributed mobile ad hoc networks (MANETs). In MANETs, providing safe communication between mobile nodes, reorganization the position of nodes, handling misbehaviour are critical issues so trust management framework play very important role in MANETs. The characteristics of mobile ad hoc networks causes a number of challenges to security design such as lack of infrastructure, shared wireless medium, stringent resource constraints and highly dynamic topology. The inherent freedom in self-organized mobile adhoc networks (MANETs) introduces challenges for trust management; particularly when nodes do not have any prior knowledge of each other. Mainly, some trust management basis may be exploited to fulfill new attacks. Here, a holistic view on various trust management frameworks geared for MANETs is presented, capable to handle main existing attacks deceiving trustworthiness computation to mislead trust-based network operations, referred to as trust-distortion attacks. Besides, taxonomy of main identified trust-distortion attacks based on how the trustworthiness estimation of a node about another node is distorted is proposed. For each framework, a unified approach is used to describe the trust model, taking each component required for trust management as a guideline. Moreover, each framework is analyzed regarding its resistance against different trust-distortion attacks, the framework unique features, merits, demerits. Finally, different trust management frameworks resisting double face attacks are compared.

Index Terms—Mobile ad hoc networks, Trust Management Framework (TMF), Double Face Attacks.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) [5] are multihop wireless networks dynamically constructed by mobile nodes without the aid of any established infrastructure. MANETs are especially useful in military, communication dispatch system, on the fly collaborative computing outside the office environment and other tactical applications such as emergency rescues. In a MANET nodes should collaborate with each other to support the functions of the network. However, because of the self-organized nature and insufficient resources, the nodes in a network can misbehave and behave selfishly for individual interests (e.g., misroute packets). To force nodes in MANETs to obey the protocol and cooperate with each other in a normal way, the trust management framework has attracted much research attention. Although the trust management enables nodes to fulfil interactions only with trusted nodes, such a framework may be menace by attackers exploiting the trust management inherent properties. Such attackers endeavour to deceive nodes estimation on other nodes trustworthiness, denying the trust management functionality. Consequently, a trust management framework should particularly care of such trust-distortion attacks. A current survey shows [1][2][6] that trust management frameworks dealing with trust-distortion attacks has not been provided. So a holistic view of existing trust management frameworks able to cope with trust-distortion attacks is provided. For each such framework, mainly emphasize is given on the mechanisms and approaches taken for each of its trust management components. Also focus is given on knowledge collection component, trust computation component and trust establishment component used in trust management frameworks resisting double face attacks. Outline of paper is as follows. Section II explains related works. Section III presents various double face attacks. Section IV emphasis on different TMFs resistant to double face Attacks dealing with which approach is used , corresponding advantages and disadvantages. Table I shows this comparative study. Finally, section V concludes the paper.

II. RELATED WORK

In network security, trust is interpreted as a set of relations among nodes participating in the network activities [3]. Trusted relationships among nodes in a network are based on different sources of information such as direct interactions, witness [7] information and previous behaviours of nodes. Trust management in distributed and resource-constraint networks, such as disconnected mobile ad-hoc networks (MANETs) is much more difficult but more crucial than in the traditional hierarchical architectures, such as the Internet and access point centred wireless LANs. Generally, this type of distributed network has neither pre-established infrastructure, nor centralized control servers or trusted third parties. The dynamically changing topology and intermittent connectivity of disconnected MANETs establish trust management more as a dynamic systems problem [8]. A selfish node may attempt to save its battery through dropping data packets or even refusing to forward routing packets to avoid paths from it. Malicious attackers may announce good routes via themselves to deny network services for following data packets, e.g. by dropping or modifying such packets. Consequently, a trust management framework is particularly required in MANETs, providing nodes with mechanisms to generate, manage, and exchange trust information, punish selfish/ malicious behaviors and encourage the cooperation in the network. A Trust Management Framework consists of three main components: knowledge collection, trust level computation and trust establishment. The knowledge collection component provides the information about node's behavior. The behavioral data can be obtained from local or both local and remote sources. The local knowledge consists in information nodes have collected by themselves on the behaviour of their neighbours. The remote information, referred to as recommendations, consists in the opinion of other nodes about the trustworthiness of a given node. The computation component calculates a trust level for each entity based on the collected behavioural data [18] or trust evidence. The result is the assignment of a trust level, representing how much a node can trust in others. The trust establishment component infers if a node can be trusted based on its trust level. Jin-Hee Cho [1] provided an overview on various potential attacks like Routing loop attacks, Worm hole attacks, Black hole attacks, Gray hole attack, Denial of Service (DoS) attacks, False information or false recommendation, Incomplete information, Packet modification /insertion, Newcomer attacks, Black mailing, Replay attacks, Sybil attacks, Selective misbehaving attacks in MANETs. Depending on design mode J. Cho [1] explained trust management scheme like secure routing, authentication, intrusion detection, access control, key management, and trust evidence distribution and evaluation etc. irrespective of different trust components. Therefore, this survey does not allow differentiating and comparing among different existing solutions. So we mainly propose a classification of trust-distortion attacks which mainly focus on different trust management frameworks resisting double face attacks. K. Govindan and P. Mohapatra provided various trust computing approaches geared towards MANETs [9]. According to [9] trust computations are broadly classified into two categories as Distributed trust computations and Centralized trust computations. Distributed trust computations can be classified as Neighbour sensing trust (Direct Trust), Recommendations based trust (Indirect Trust), and Hybrid trust (combination of both direct and indirect trust). Centralized trust establishment assumes a Trust Agent (TA) which can be accessible by all nodes in the group. Here the Trust Agent either computes the trust for the whole community or assists the nodes in their trust computations by providing the initial trust values on target nodes. K. Govindan analyzed the techniques proposed for different trust dynamics including trust propagation, prediction and aggregation algorithms, as well as the impact of trust on security services. Although this work describes different approaches that can be used to design each trust management component separately, it does not provide a holistic view of components used by each trust management scheme. Renu Dalal [2] classified different trust management frameworks into five groups: protocol based, system level based, cluster based, maturity based and Public Key Infrastructure (PKI) based. However, the proposed categories are based on so common characteristics that make every framework appropriate to almost all categories. Moreover, the paper does not utilize a unified approach to describe each trust management framework and to detail the mechanism used by each of its components. Finally, the paper does not emphasize different trust-distortion attacks. Here we provide detailed study of numerous techniques resisting mainly double face attacks.

III. DOUBLE FACE ATTACKS

On the basis of how the attack distorts the trustworthiness estimation of a node about another node trust distortion attacks are classified into double face attacks and bad mouthing. Here we focus on double face attacks only. Double face attack consists in performing misbehaviour actions so that the attacker can remain undetected. To achieve this, such an attacker may disperse its attack over time, switch between good and bad actions alternatively, or/and target a particular user or a particular network region in order to deceive nodes perception on other nodes' behaviour. Double face attacks are classified into on-off and conflicting behaviour attacks based on whether the threat is temporally or spatially distributed.

On-off double face attacks:

In on-off double face attack, bad actions are temporally dispersed in order to adjust the trustworthiness level of an attacker calculated by other nodes above the misbehaviour threshold. This latter is performed through

switching alternatively between misbehaviour (on) and normal (off) conducts to remain undetected while causing damage. Again on-off double face attacks are classified into detonator and iterative attacks.

Detonator on-off double face attack:

In a detonator on-off attack, an attacker starts misbehaviour actions after a period of time of normal behaviour and remains in new status forever [10].

Iterative on-off attack double face attack:

Iterative on-off attack consists in the generalized form of detonator on-off attack in which an attacker switches iteratively to normal conduct after a certain period of misbehaviour actions. To deal with the time-domain dispersion of on-off attacks and track the resulted trustworthiness level dynamics, the past negative experiences should not be forgotten as quickly as past normal observed actions. The most commonly used technique is to introduce an adaptive forgetting factor inspired from human's behavior, which remembers bad behaviors for a longer time than they do for good behaviours. The advantage of the adaptive forgetting factor is that when an entity turns bad, the trust value can keep up more quickly with the entity's current status.

Conflicting Behavior double face Attack:

In conflicting behaviour attack, an attacker node behaves selfishly in a position (or regarding a node) and normally in another position (or regarding another node) in order to remain undetected [11]. We classify conflicting behavior attacks into position-domain and user-domain attacks.

Position-domain conflicting behaviour double face attack:

It is concerned with a particular region in the network. In position-domain conflicting behaviour attack, malicious entities can perform bad actions in the target position and then move to another position conducting normal or abnormal actions. Since the nodes located in new position do not have any previous judgment about that attacker's malicious nature, they will interact with it during the detection time. To address this issue, a trust propagation mechanism distributing recommendations all over the network allows nodes to timely detect such attackers wherever in the network.

User-domain conflicting behaviour double face attack:

It is concerned with a particular user (or group of users). In user-domain conflicting behaviour attack, an attacker behaves well to all users except a particular user (or group of users) to cause them developing conflicting opinions about the malicious node. In such a case, if node's trustworthiness is based only on local information, non-victim nodes remain unaware of the attack, leaving the victim node to face the attacker lonely. However, when recommendations are utilized, the conflicting opinion received from a victim node may lead the evaluator node to distrust the victim node. Consequently, the attacker can keep its trustworthiness level at a high value regardless of its misbehaviors. Meanwhile, the nodes under attack can be excluded from the network [11]. A simple way to detect this kind of attack consists in using the trustworthiness level of recommender to judge about such conflicting behaviours.

IV.DIFFERENT TMFS RESISTANT TO DOUBLE-FACE ATTACKS

1 Global Reputation Table (GRT) based TMF

In this Trust management framework Global Reputation Table (GRT) [12] is used to store the node's view on neighbours and far nodes. A node uses the received recommendations to update its GRT table before rebroadcasting it to its neighbours after a predefined schedule. The new value of a neighbour trustworthiness in GRT is calculated as the weighted sum of its local reputation (if a neighbour node), its current reputation value in GRT and the received remote value. GRT based TMF is resistant to only detonator on-off attack and conflicting behaviour attack. But it is not resistant to iterative on-off attacks because no mechanism is provided to maintain attackers misbehaving history. Also GRT based TMF is vulnerable to the bad mouthing attack since no mechanism is considered to differentiate between correct and false recommendations. Although the efficiency of this system has been proved with respect to detonator on-off attack, this proposal is not immune to iterative on-off conduct. To solve this issue, GRT based TMF should consider a mechanism for maintaining attackers misbehaving history so that the re-trust to such an attacker takes place only after a relevant period of good behaviour. For any return to misbehaviour mode, an observer node should stretch out the required period the attacker should behave trustworthy to be able to be re-trusted. Moreover, It [12] is vulnerable to the bad mouthing attack since no mechanism is considered to differentiate between correct and false recommendations. Furthermore, we believe that the framework gets also immune to the conflicting behaviour attack since nodes' trustworthiness is evaluated based on both positive and negative recommendations received from all over the network. Indeed, remote nodes are warned through received recommendations and would relinquish interacting with attacker nodes. Limitations of GRT based TMF is that the detection of a local misbehaviour may become a time-consuming process, especially when the network traffic is light. If the attacker drops packets of a particular

next hop, the victim node cannot detect this behaviour. Finally, the old-age algorithm may erroneously punish a normal node.

2 KMAPE (Knowledge, Monitor, Analyse, Planning and Execution) based TMF

It is [13] Autonomic Trust Knowledge Monitoring Scheme involving various components like knowledge, Monitor, Analyse, Planning and Execution. The Knowledge Component consists in a knowledge base, which includes Local Trust Table (LTT) and Global Trust Table (GTT). The policies allow the framework to analyze its current state and adjust its monitoring rate accordingly. The Analyzing Component periodically verifies if any predefined policies threshold is exceeded considering the knowledge provided by the monitor component. If this is the case, it activates the planning component in order to react to that event. The Planning Component executes the knowledge monitoring optimization algorithm when the traffic rate exceeds a congestion threshold. The Execution Component is responsible for enforcing decisions taken by the planning component. The main asset of KMAPE based TMF is the self-adaptation of its knowledge collection component. It optimizes the network monitoring cost. KMAPE based TMF is not resistant to bad mouthing attack because it does not consider any mechanism to distinguish between correct and false recommendations. Also it is not resistant to iterative on-off attack.

3 RREP (Route Reply) based TMF

In the knowledge collection component [4], successful and unsuccessful interactions of neighbours are gathered. To collect the indirect information, the intermediate nodes piggyback their trust table in routing packets. This information is received by the original source through Route Reply (RREP) packets and used to evaluate the trustworthiness of nodes on the path. In the trust level computation component, a node's trust value is increased by one when a good behaviour is observed and decreased by a value proportional to the observer node's policy when a misbehaviour is detected. When the node's trust value attains 0, it is considered as malicious. RREP based TMF can resist the user-domain conflicting behaviour attack since the trust value of nodes on the path is available at the source. Also it is capable to face the on off attack. But RREP based TMF is vulnerable to the bad mouthing attack since no mechanism is defined to detect false recommendations. Also it is vulnerable to position-domain conflicting behaviour since recommendations are not propagated all over the network.

TABLE I
Comparison of Different Trust management Frameworks resistant to Double Face attacks

Sr. No.	Name of author	Approach used	Knowledge collection component	Trust computation component	Trust establishment component	Features	Limitations
1	G. Bella, G. Costantino[12]	GRT (Global Reputation table)	Local and Remote current reputation value in GRT and the received remote value	Forwarded traffic	None	Resistant to only detonator on-off attack and conflicting behaviour attack	No mechanism is provided to maintain attackers misbehaving history. It is not resistant to iterative on-off attacks. Detection of a local misbehaviour is time consuming process.
2	Z. Movahedi, M. Nogueira[13]	KMAPE	Local Trust Table (LTT) and Global Trust Table (GTT)	Generated traffic	None	Self-adaptation of its knowledge collection component. It optimizes the network	Not resistant to iterative on-off attack. Can't distinguish between correct and false recommendations

						monitoring cost.	
3	S. Almotiri and I. Awan, [4]	RREP	Local and remote	Successful and unsuccessful interactions of neighbours	Route With highest trust value	Resist the user-domain conflicting behaviour attack. Capable to face the on off attack.	Vulnerable to position-domain conflicting behaviour. No mechanism to detect false recommendations.
4	S. Bansal and M. Baker [14]	OCE	Direct information	Ratings value	Faulty-list to the route request (RREQ) message	Does not suffer from false rating. Saves local memory. It is resistant to detonator on-off attack	It cannot resist the user-domain conflicting behaviour attack
5	Guo Jianli [15]	HCE	Direct information	Ratings value	Faulty-list and selfish-list	It is resistant to detonator on-off attacker.	Cannot resist the user-domain conflicting behaviour attack
6	Antesar M. Shabut [16]	CR	Direct and indirect trust information	Bayesian statistics	Number of interactions by the means of using confidence value	It is resistant to on-off attacks and bad mouthing attack	Cannot resist the user-domain conflicting behaviour attack

4 OCE (Observation Cooperation Enforcement) based TMF

OCE based TMF uses only direct [14] that is first-hand observations. Every node in the networks maintains a ratings value for each of its neighbouring nodes. Once the rating of a node falls below a certain faulty threshold, the node is added to a faulty-list. When the node takes part in the route discovery process, it attaches the faulty-list to the route request (RREQ) message. OCE based TMF cannot give accurate detection on the monitored node. It introduces the second chance mechanism. After a fixed period of inactivity, the misbehaving node is removed from the faulty-list. It uses a simple credit-based model to deal with nodes that do not participate in the route discovery process. Node keeps one counter, called chip-count, for each neighbour. Advantages of OCE based TMF are as follows. It does not suffer from false rating. Since OCE based TMF only uses the first hand information and does not use the indirect second hand information. It saves local memory. Also it saves bandwidth. In this scheme nodes do not broadcast any control messages. This scheme can enforce the selfish nodes to cooperate. It is resistant to detonator onoff attacker as soon as it begins its permanent attack phase .But it is not resistant to on-off attack. Also it cannot resist the user-domain conflicting behaviour attack except in a situation where a node wants to establish a path including the misbehaviour node and the victim node.

5 HCE (Hybrid Cooperation Enforcement) based TMF

It is a hybrid cooperation enforcement in mobile ad hoc networks) to make the misbehaviour unattractive. It [15] is an improvement to OCEAN (observation- based cooperation enforcement in ad hoc networks). It employs only first hand information and works on the top of DSR (dynamic source routing) protocol. By interacting with the DSR, HCE based TMF can detect the misbehaviour nodes in the packet forwarding process and isolate them in the route discovery process. In order to detect the misbehaviour nodes quickly, this scheme introduces the warning message. In HCE based TMF, each node has a unique, persistent, and distinct identity and knows its

one-hop neighbours. Transmission distance of each node is the same. Links between nodes are bidirectional. Nodes do not have a priori trust relationship. On demand routing protocols such as DSR, are used to establish route. Misbehaviour nodes like malicious nodes, misleading nodes, and selfish nodes can be detected by this scheme, and isolated from the network. The watchdog locating at each node keeps a faulty-list and a selfish-list. All the neighbour nodes detected as malicious or misleading are put into the faulty-list, whereas the neighbour nodes considered as selfish are put into the selfish-list. Before deciding whether to forward the packet for a neighbour, the node checks its faulty-list and selfish-list. If the neighbour lies in its faulty-list or selfish-list, the node denies the request. HCE based TMF also keeps a reputation table in each node, with each row corresponding to a neighbour node. Each node broadcasts the warning message to its neighbours in a period, putting its faulty-list and none chip-list into it. Each time, a node receives a warning message from one neighbour, updates the avoid-list and none chip-list corresponding to the sending node in the reputation table, substituting with the faulty-list and selfish-list in the warning message. The receiver does not rebroadcast the warning message again. This scheme employs the second chance mechanism. It allows nodes previously considered misbehaving to become useful again. A timeout approach is used where a misbehaving node is removed from the faulty-list after a fixed period of inactivity. Even though the node is removed from the faulty-list, its rating is not increased, so that it can quickly be added back to the faulty-list if it continues the misbehaviour. It is resistant to detonator on -off attacker as well as on-off attack. Its rating is not increased, so that it can quickly be added back to the faulty-list if it continues the misbehaviour.

6. CR (Clustered Recommendation) based TMF

CR based TMF is used to filter out attacks related to dishonest recommendations like bad-mouthing, ballot-stuffing, and collusion for mobile ad hoc networks. Recommendations are accumulated over a period of time to ensure the consistency of recommendations provided by a recommending node regarding the evaluated node. Clustering [16] technique is adopted to dynamically filter out recommendations between certain timeframe. This scheme uses a Bayesian statistical approach similar to that used in [17] for computing trust values based on the assumption that they follow a beta probability distribution. CR based TMF clusters recommendations based on three different criteria: (a) number of interactions by the means of using confidence value, (b) compatibility of information with the evaluated node by the means of deviation test, and (c) closeness between these nodes. The use of multiple criteria to judge whether a node is dishonest can mitigate the influence of false negative and false positive ratings. Furthermore, the neighbourhood relationships between nodes are better predicted and identified using the multiple criteria. The model has three components deployed to evaluate trust: (a) Trust Computation Component that uses direct as well as indirect (second hand) trust information. (b) Recommendation Manager Component that requests and gathers recommendations for a node from a list of recommending nodes, and (c) Cluster Manager Component which filters out dishonest recommendations from the list and sends out a list of trustworthy recommendations to the manager component. It is resistant to on-off attacks and bad mouthing attack. TABLE I shows comparison of Different Trust management Frameworks resistant to double face attacks.

VI. CONCLUSION

Trust management plays very important role in handling different types of attacks. A hierarchy of main trust-distortion attacks is provided. Main categories are double-face and bad mouthing attacks .Here we focus on double face attacks and relative trust management framework handling particular trust distortion attack. Here we identified six main trust management frameworks for handling double face attacksas follows: GRT (Global Reputation Table) based TMF, KMAPE (Knowledge, Monitor, Analyse, Planning and Execution) based TMF, RREP (Route Reply) based TMF, OCE (Observation Cooperation Enforcement) based TMF, HCE(Hybrid Cooperation Enforcement) based TMF, CR (Clustered Recommendation) based TMF. Finally comparison of above trust management frameworks is done as shown in TABLE I considering approach used, knowledge collection component,Trust computation component, Trust establishment component, features and limitations.

REFERENCES

[1] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 562–583, Nov. 2011.
[2] R. Dalal, M. Khari, and Y. Singh, "Different ways to achieve trust in MANET," Int. J. AdHoc Netw. Syst. (IJANS), vol. 2, no. 2, pp. 53–64, Apr. 2012.
[3] S. Lim Choi Keung and N. Griffiths, " Building a Trust-based Social Agent Network," in Proceedings of the 12th International Workshop on Trust in Agent Societies, pp. 68-79, 2009.
[4] S. Almotiri and I. Awan, "Trust routing in MANET for securing DSRrouting protocol," PGNet, 2010.
[5] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[6] R. Dalal, M. Khari, and Y. Singh, “Survey of trust schemes on adhoc network,” in Advances in Computer Science and Information Technology. Networks and Communications, N. Meghanathan, N. Chaki, and D. Nagamalai, Eds. New York, NY, USA: Springer, 2013, pp. 170–180.
[7] S. D. Ramchurn, D. Huynh, and N. R. Jennings, “Trust in multi-agent systems,” Knowl. Engg. Rev., Vol. 19, No. 1, pp. 1–25, 2004.
[8] John S. Baras, Tao Jiang, "Managing Trust in Self-organized Mobile Ad Hoc Networks" in the 12th Annual Network and Distributed Sys. Security Symposium (NDSS) workshop, San Diego, February 2005.
[9] K. Govindan and P. Mohapatra, “Trust computations and trust dynamics in mobile adhoc networks: A survey,” IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279–298, May 2012.
[10] M. Morvan and S. Sene, “A distributed trust diffusion protocol for ad hoc networks,” in Proc. Int. Conf. Wireless Mobile Commun. (ICWMC), 2007, pp. 87–92.
[11] J. Li, R. Li, and J. Kato, “Future trust management framework for mobile ad hoc networks,” IEEE Commun. Mag., vol. 46, no. 4, pp. 108–114, Apr. 2008.
[12] G. Bella, G. Costantino, and S. Riccobene, “Managing reputation over MANETS,” in Proc. 4th Int. Conf. Inf. Assur. Security (IAS), 2008, pp. 255–260.
[13] Z. Movahedi, M. Nogueira, and G. Pujolle, “An autonomic knowledge monitoring scheme for trust management on mobile ad hoc networks,” in Proc IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2012, pp. 1898–1903.
[14] S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks,” 2003, pp. 120–130.
[15] GUO Jianli , LIU Hongwei , DONG Jian , YANG Xiaozong ,“HEAD: A Hybrid Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” Tsinghua Science And Technology ISSN 1007-0214 36/49 pp202-207 Volume 12, Number S1, July 2007
[16] Antesar M. Shabut, Keshav P. Dahal, Senior Member, IEEE, Sanat Kumar Bista, and Irfan U. Awan, “Recommendation Based Trust Model with an Effective Defence Scheme for MANETs,” IEEE Transactions On Mobile Computing, Vol. 14, No. 10, October 2015
[17] A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” Decision Support Syst., vol. 43, no. 2, pp. 618–644, 2007.
[18] John S. Baras, Tao Jiang, "Managing Trust in Self-organized Mobile Ad Hoc Networks" in the 12th Annual Network and Distributed Sys. Security Symposium (NDSS) workshop, San Diego, February 2005.