VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

A SURVEY ON ISOLATION OF BLACKHOLE ATTACK USING TRUST MANAGEMENT

C. Senthilkumar[1], N. Kamaraj[2] and J. Gautam[1]
[1]Department of Computer Science Engineering, Thiagarajar College of Engineering, Madurai, India
[2]Department of Electrical and Electronics Engineering, Thiagarajar College of Engineering, Madurai, India
E-Mail: cskumar2005@gmail.com

ABSTRACT

MANET is a self methodized system comprised of mobile nodes without any infrastructure. MANET are at more imperil to attacks since it is dynamic in nature. To define and manage trust in a military MANET, we must cogitate the interface between the communication networks, and severe resource constraints such as computing power, energy, bandwidth, time etc and dynamics. Dynamics include changes in topology, mobility of the node, failure of the node and conditions for propagation channel. Therefore trust in MANET plays a vital role in the performance of MANET. MANET is vulnerable to several attacks. Black Hole attack is one of the attacks that advertise it for having the shortest route to destination node and then drops the entire packet that is coming from source node. In this paper, we have reviewed different solutions against Black hole attacks in Mobile Ad-Hoc networks and thoroughly compare these schemes to find out their various advantages and disadvantages based on trust evaluation and management.

Keywords: black hole attack, AODV, trust, intrusion detection system.

1. INTRODUCTION

MANET is self configuring and distributed network. In Mobile Ad-Hoc Network nodes uses wireless links to communicate with each other on the basis of mutual trust. MANET has allure to various applications such as military, disaster recovery, personal area network and more. Each node communicates with the other acting as routers. MANET are susceptible and defenseless to malicious attack because of its features like open medium, lack of central administration, dynamic topology changes, cooperative algorithms and so on. Snooping attacks, black hole attacks, wormhole attacks, routing table overflow, packet replication, distributed DoS (DDoS)attacks, denial of service attacks(DoS), etc are various kinds of attacks to which MANET is exposed. In this paper we define black hole attacks in AODV routing protocol in mobile Ad-Hoc network. We use AODV protocol because it is widely used and vulnerable to these attacks. Security in Mobile Ad-hoc Network is considered to be the important factor for the network. Therefore, a proficient intrusion detection must be adopted to assist the identification and isolation of attacks. In this paper we have surveyed trust evaluation and management and various intrusion detection techniques in MANET against Black hole attack. Based on the information acquired, the routing protocols is classified into proactive, reactive and hybrid routing.

1.1 What is Trust?

The perception of trust is significant to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. According to Eschenauer *et al.* [1], trust is defined as "a set of relations among entities that participate in a protocol. These associations are based on the testimony engendered by the previous interactions of entities within a protocol. In broad, if the interactions have been realistic to the protocol, then trust will buildup between these nodes."Trust is outlined because the degree of belief concerning the mien of different entities [2]

1.2 Properties of Trust

Golbeck [3] discusses the three main properties of trust in the context of a social network perspective: asymmetry, personalization and transitivity. First, trust is not perfectly transitive in nature. That is, if A trusts B, and B trusts C, it does not assure that A trusts C. Second, trust is not certainly symmetric i.e, not alike in both directions. A distinctive example of asymmetry of trust can be found in the relationships between Faculties and Students. Third, trust is fundamentally a personal opinion. Two people often appraise trustworthiness about the same entity contrarily.

1.3 Characteristics of Trust in MANETs

Due to the distinctive characteristics of MANETs and unreliability of the wireless medium, the notion of trust in MANETs should be precisely defined. The main features of trust in MANETs are as follows [1,2,4 and 5]:
1. Trust is always dynamic.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

2. Trust is subjective in nature.
3. Trust is not perfectly transitive. The fact that A trusts B and B trusts C does not implies that A trusts C.
4. Trust is asymmetric and not necessarily reciprocal.
5. Trust is context-dependent.

1.4 Relation among trust, trustworthiness and risk

In the literature, the terms trust and trustworthiness seem to be interchangeably used without clear distinction. Josang *et al.* [6] clarified the difference between trust and trustworthiness based on their definitions provided by Gambetta [7]. The level of trust is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust) [6]. In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected. Solhaug *et al.* define trustworthiness as the objective probability that the trustee performs a particular action on which the interests of the trustor depend. Figure-1 [8] defines how trust and trustworthiness differs and how the difference affects the level of risk the trustor needs to take. In Figure-1, the diagonal raced line is considered to be trail of well-defined trust in which the subjective probability of trust (i.e., trust) is equivalent to the objective probability (i.e., trustworthiness). Depending on the extent to which the trustor is ignorant about the difference between the believed (i.e., trust) and the actual (i.e., trustworthiness) probability, there is uncertainty or a miscomputation of the involved risk. In other words, the subjective aspect of trust gives inaccurate risk estimation and untrue risk management accordingly. Figure-1 implies cases where probability is miscomputed. In the part below the diagonal line, there is mislaid trust to assorted degrees that the obtained trust is greater than the actual trustworthiness. Though risk is an intrinsic property of trust, even well-estimated trust, mislaid trust increases risk and thus the chance of deceit, as shown in the example marked with a and b in Figure-1.

2. TRUST MANAGEMENT IN MANET

The concept of "Trust" initially derived from social sciences and is defined as the degree of subjective belief about the manners of a precise entity [9]. Blaze *et al.* [10] first introduced the term "Trust Management" and specified it as a separate element of security services in networks and cleared that "Trust management provides a incorporated approach for specifying and interpreting security policies, relationships and credentials" Trust management in MANETs is required when participating nodes, without any prior interactions, craving to establish a network with an adequate level of trust relationships among themselves. Examples would be in establishing initial trust bootstrapping [11], league operations without predefined trust, and authentication of certificates generated by third party when links are down or ensuring safety before introducing a new zone [12 Added, resource constraints often narrow the trust evaluation process only to local information. The dynamic characteristic of MANETs result in ambiguity and incompleteness of the trust evidence, which continuously changes over time [12] [13]. Despite a couple of surveys of trust management [14], a comprehensive survey of trust management in MANETs does not exist [14].

2.1 Existing trust management in MANETs

Trust management designs have been developed for specific purposes such as secure routing, intrusion detection, access control (authorization) and authentication.

Trust evidence distribution and evaluation

Several trust management schemes have been projected in order to provide a general framework for trust evidence distribution or evaluation in MANETs. Jiang and Baras [15] proposed a trust distribution design called ABED (Ant-Based trust Evidence Distribution) based on the swarm intelligence paradigm, which is claimed to be vastly distributed and adaptive to mobility. The swarm intelligence paradigm is broadly used in dynamic optimization problems such as traveling salesman problem, routing in communication networks and is inspired from artificial ant colony techniques to elucidate combinatorial optimization problem.

The odorakopoulos and Baras [15] proposed a trust evidence evaluation design for MANETs. The evaluation process is sported as a path problem in a directed graph where nodes specifies the entities and edges specifies trust relations. The authors employ the theory of Semirings to illustrate how two nodes can establish trust relationships lacking prior direct interactions. Their case study uses the GP web of trust to articulate an example trust model based on Semirings and shows that their proposed design is robust in the presence of attackers. Still, their work considers that trust is transitive. Further, trust and confidence values are signified as binary rather than as a continuous-valued variable. Though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure.

Recently Buckerche and Ren [16] proposed a distributed reputation evaluation prototype called GRE (Generalized Reputation Evaluation) to efficiently preclude malicious nodes from entering the trusted community. However, no specific attack model was addressed.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

3. DESIGN CHALLENGES IN MANET

A mobile ad hoc network [18] encompass wireless mobile nodes casting a transitory network without the assistance of centralized infrastructure, and where nodes communicate amongst multi-hops. Security protocol orginators for MANETs experience technical challenges due to severe resource constraints in bandwidth, battery life, memory size, exclusive and computational power. Wireless characteristics such as openness to eavesdropping, lack of specific ingress and exit points, high security threats, unreliable communication, vulnerability and rapid changes in topologies due to user mobility or node failure [18],[19].

4. BLACK HOLE ATTACK

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviours because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. Trust relationship between the nodes play a significant role in isolating the malicious nodes that roots a black hole attack in the network. A malicious node, the so called black hole node, may always respond positively to route requests even when it does not have proper routing information. The black hole can drop all packets forwarded to it. In other words Black Hole attack is one of the attacks that advertise it for having the shortest path to destination node and drops the entire packet that is coming from source node [17]. Node 3 is a misbehaviour node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneouslyjudges the route discovery process with completion, and starts to send data packets to node 3.

4.1 Single Black hole attack

In this type of attack, one malicious node drops the routing packets which it is supposed to forward to its neighbours by claiming itself of being shortest path to destination node by the routing protocol. For instance, consider node 3 to be a black hole node that drops the packets sent from the source which is supposed to be forwarded. Initially source 1 broadcasts a route request message to send packets to destination. At first, the node 3 claims that it has the shortest path to the destination and generates a false RREP message to the source before the actual RREP reaches the source node. And so the source started to send the packets to destination through node 3.

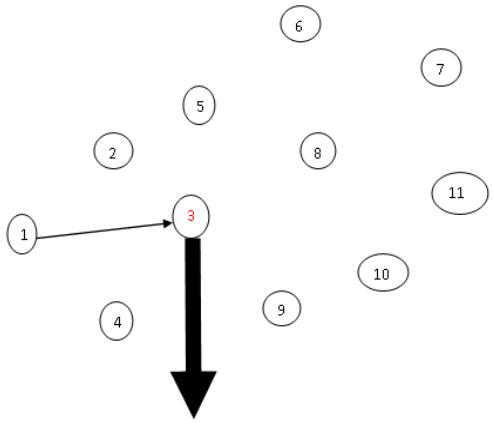

Figure-1. Packet drop by black hole node

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

4(a). Comparison of Single Black hole attack detection schemes based on trust evaluation.

Proposed method	Routing protocol	Tool used	Type of detection	Year of publication	Inference	Defects
Routing discovery based on neighbourhood discovery [20]	AODV	NS-2	Single Detection	2003	The probability of one attacker can be inferred is 93%	Failed when attackers cooperate to forge the fake reply packets.
Unique sequence number and Redundant route scheme [21]	AODV	NS-2	Single Detection	2004	Routes are verified around 75% to 80%	Attackers can monitor the channel and update the tables for last sequence number
Detection scheme based on time threshold [22]	Secure AODV (SAODV)	GloMoSim	Single Detection	2007	The PDR of SAODV is around 90 to 100% when AODV is around 80%	The end-to-end delay increases when the distance between malicious node and source node increases
Bayesian Detection scheme based on Random Two-hop ACK [23]	DSR	GloMoSim	Cooperative Detection	2007	The true positive rate can acquire 100% at instance of 2 witness	The proposed method should be enhanced when k equals to reducing the true positives
REAct [24]	DSR		Single Detection	2009	Minimizes the communication overhead but enhances the identification delay	The binary search method is easily expose audit node's information
DPRAODV [25]	AODV	NS-2	Single Detection	2009	The PDR is enhanced by 80 to 85% than AODV in the presence of Black hole attack	A little bit higher routing overhead and delay than AODV

5. CONCLUSIONS AND FUTURE WORK

In this paper, we surveyed and analyzed existing trust management schemes in MANETs to provide MANET trust network protocol designers with multiple perspectives on the concept of trust, an understanding of trust properties that should be observed in developing trust metrics for evaluating trust, and insights on how a trust metric can be customized to meet the requirements and goals of the targeted system. We also analyzed the effect of types of Black Hole Attack in the network and the significance of trust management to eliminate the Black hole attack that provides the protocol designers a perspective view on the significance of trust evaluation and management. The proposed methods to detect and isolate black hole attacks are subjected to various defects which could probably reduce the Quality of Service in an ad-hoc environment. This issue can be minimized with the concept of trust evaluation and management. A trust value for each node based on the QoS parameters such as packet drop ratio, end to end delay etc should be computed. Energy of the node is also taken into account. When the packet drop ratio more than a threshold value in a fixed path, the path must be recomputed based on the trust value computed i.e, the node with the maximum trust value. This new path to destination would contain only the nodes with a decent trust value which probably leads to a improved quality of service.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

REFERENCES

[1] L. Eschenauer, V. D. Gligor and J. Baras. 2002. "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. Vol. 2845, pp. 47-66.

[2] L. Capra. 2004. "Toward a Human Trust Model for Mobile Ad-hoc Networks," Proc. 2nd UK-UbiNet Workshop, 5-7 May, Cambridge University, Cambridge, UK.

[3] J. Golbeck. 2006. "Computing with Trust: Definition, Properties, and Algorithms,"Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks, Baltimore, MD, 28 August – 1 September. pp. 1-7.

[4] W. J. Adams, N. J. Davis. 2005. "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW'05), 15-17 June, West Point, NY, pp. 317-324.

[5] Y. L. Sun, W. Yu, Z. Han and K. J. R. Liu. 2006. "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, no. 2, February. pp. 305-317.

[6] Josang and S. LoPresti. 2004. "Analyzing the Relationship between Risk and Trust," Proc. 2nd Int'l Conf. Trust Management (iTrust'04), LNCS, Springer-Verlag, pp. 135-145.

[7]J. Li, R. Li, and J. Kato. 2008. "Future Trust Management Framework for Mobile AdHoc Networks: Security in Mobile Ad Hoc Networks," IEEE Communications Magazine, Vol. 46, no. 4, April. pp. 108-114.

[8] Solhaug, D. Elgesem and K. Stolen. 2007. "Why Trust is not proportional to Risk?" Proc. 2nd Int'l Conf. on Availability, Reliability, and Security (ARES'07), 10-13April, Vienna, Austria, pp. 11-18.

[9] K. S. Cook (editor), Trust in Society, Vol. 2, Feb. 2003, Russell SageFoundation Series on Trust, New York, USA.

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

[11] R. B. Bobba, L. Eschenauer, V. Gligor and W. Arbaugh. 2003. "Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks,"Proc. IEEE GLOBECOM, San Francisco, CA, Dec. pp.1511-1515.

[12] L. Eschenauer, V. D. Gligor and J. Baras. 2002. "On Trust Establishmentin Mobile Ad Hoc Networks," Proc. 10th Int'l Security ProtocolsWorkshop, Cambridge, U.K., Apr. Vol. 2845, pp. 47-66.

[13] J. S. Baras and T. Jiang. 2005. "Managing Trust in Self-Organized MobileAd Hoc Networks," Proc. 12th Annual Network and Distributed SystemSecurity Symposium Workshop, February. San Diego, CA.

[14] S. Ruhomaa and L. Kutvonen. 2005. "Trust Management Survey," P. Herrmann *et al*. (Eds.), iTrust, Lecture Notes in Computer Science, Vol. 3477, pp. 77-92.

[15] Theodorakopoulos and J. S. Baras. 2006. "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, no. 2, February. pp. 318-328.

[16] Boukerche and Y. Ren. 2008. "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada, pp. 88-95.

[17] Y. Hu and A. Perrig. "A Survey of Secure Wireless Ad Hoc Routing,

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

[19] J. Jubin and J. Tornow. 1987. "The DARPA Packet Radio Network Protocols," Proc. IEEE, Vol. 75, no. 1, January. pp. 21-32.

[20] Sun B, Guan Y, Chen J and Pooch UW. 2003. Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April.

[21] Al-Shurman M, Yoo S-M and Park S. 2004. Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42ndAnnual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April.

[22]Tamilselvan L. and Sankaranarayanan V. 2007. Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August.

[23] Djenouri D. and Badache N. 2008. Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing Vol. 8, no. 6, pp. 689–704. doi: 10.1002/wcm.v8:6.

[24] Kozma W. and Lazos L. 2009. REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March.

[25] Raj PN and Swadas PB. 2009. DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science Vol. 2: pp. 54–59. doi: abs/0909.2371