Journal of Engineering and Applied Sciences 13 (6): 1425-1429, 2018
ISSN: 1816-949X

Data Plane Security Solutions in a Mobile Ad Hoc Network: A Survey

[1]Shirina Samreen and [2]M.A. Jabbar
[1]CVSR College of Engineering,
[2]Vardhamam College of Engineering,
Jawaharlal Nehru Technological University (JNTUH), Hyderabad, India

Abstract: A detailed survey upon the different approaches used to design the data plane security solutions of a Mobile Ad Hoc Network (MANET) is presented in this study. To ensure reliable data transmission from a sender node to a reciever node in a MANET, cooperation of each of the intermediate nodes forming the path towards packet forwarding is mandatory, since, it is multi-hop communication. The approaches employed for reliable data delivery will either perform node stimulation towards cooperation through rewards or perform enforcement through a punishment strategy. Specific research carried out in each category are discussed along with the advantages and disadvantages of each approach which facilitate in forming the design considerations of a data plane security solution.

Key words: Data plane security, mobile ad hoc network, cooperation stimulation, cooperation enforcement, communication, advantages and disadvantages

INTRODUCTION

The reliability of data transmission in a Mobile Ad Hoc Network (MANET) can be effected by the inherent characteristics like the dynamic topological changes in network and energy-constrained nodes due to limited battery power which result in link breaks. An estimate of reliability in MANET environment has been addressed by Pouyan and Tabari (2014). Research efforts focusing towards the problems caused as a result of the energy-constrianed property of MANET nodes (Taghizadeh and Mohammadi, 2013) have been carried out.

From the security perspective in a MANET, a broad taxonomy of attacks, considering the elements of network which are being effected is as follows. Control plane attacks and data plane attacks. The former focuses upon the working of the routing protocol and the latter focuses upon forwarding mechanisms. Accordingly, the security mechanisms designed for MANETs counter the attacks either upon the control plane or the data plane.

Packet drop attack is one of the most provocative data plane attacks which is launched following the secure route establishment. The behavior wherein an adversary on the source to destination route does not perform packet forwarding and and instead drops a packet is termed as byzantine behavior. It was first defined by Perlman (2000). Network failures can be broadly categorized as simple failure and byzantine failure. The former involves a component which simply becomes inoperative and the latter involves a component which becomes faulty but continues to research wrongly. The following are the examples of Byzantine behavior propagation of false routing information, redirection of routes and simply dropping packets. Byzantine behavior can be countered through a protocol which protects against the data plane attacks. A security mechanism which guarantees the secure forwarding of the data packets from source to destination is required to counter the data plane attacks.

MATERIALS AND METHODS

Classification of data plane security solutions: Data plane security mechanisms in a MANET can be classified into the following types according to the approach to counter the packet dropping:

- Cooperation stimulation approach or prevention approach
- Cooperation enforcement approach or punishment approach

Figure 1 shows taxonomy of data plane security. The basic difference between the two mechanisms is as follows. The distinction between rational and irrational packet droppers cannot be made by cooperation stimulation approach. By default, it assumes that selfishness for preserving the resources is the reason for packet drops. So, it performs tries to stimulate the

Corresponding Author: Shirina Samreen, CVSR College of Engineering, Jawaharlal Nehru Technological University (JNTUH), Hyderabad, India

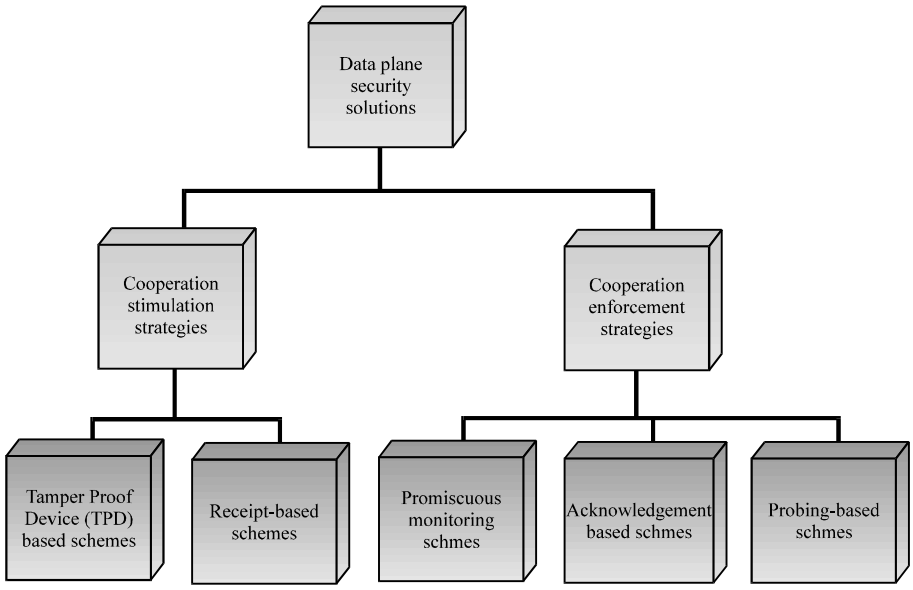

Fig. 1: Taxonomy of data plane security solutions

nodes for cooperation to perform data forwarding in the form of credits/virtual currency. Hence, it adopts an approach which tries to avoid the problem of packet dropping.

Cooperation enforcement approach makes an implicit assumption of an obligatory requirement of each node with respect to packet relay and employs a punishment approach which performs the detection of packet dropping initially and then punishment/penalty is imposed. Behavioral monitoring of the nodes assists in distinguishing between malicious and non-malicious packet dropping. The results generated are utilized by a trust/reputation framework, so as to compute a trust metric for each node which can be used to decide upon the network services.

Classification of cooperation stimulation schemes: This study will discuss about taxonomy of cooperation stimulation schemes.

Cooperation stimulation mechanisms have the intermediate nodes rewarded in terms of credits for providing the packet relay service to the source and destination nodes. The communicating source and destination nodes are accounted for utilizing the packet forwarding services of the intermediate nodes.

A deeper classification of cooperation stimulation schemes according to the resource requirements is as follows:

- Schemes based upon a Tamper Proof Device (TPD)
- Schemes based upon cryptographically generated Receipt

Tamper Proof Device schemes (TPDS): These schemes have nodes with a TPD installed within them, so as maintain node credits acquired through packet forwarding. A scheme called as Secure Incentive Protocol (SIP) (Zhang *et al*., 2007) utilizes special packets called as RECEIPT packets and REWARD packets. A RECEIPT packet is sent by the destination causeing the issue of a REWARD packet by the source node. This results in an increment of the credit accounts of each of the the intermediate nodes on the source to destination path. CASHnet (Weyland and Braun, 2004) is researcher scheme wherein the credit accounts of the communication source and the destination nodes are charged for packet transmission.

Limitations associated with the TPD schemes are as follows. The assurance with respect to tamper-free TPD cannot be provided due to the fact that MANET is an open network involving autonomous nodes which can be easily captured by external attackers. The necessity of sufficient credits, so as avail network services creates problems for those nodes which could not offer forwarding service for other nodes as they did not fall in the source to destination route. In a MANET environment which comprises link breaks due to mobility of nodes or noise in the channel, it has been shown by Weyland *et al*. (2006) that a gradual deterioration of the overall credits of the nodes in the network occurs with TPD-based schemes, since, the total charges may exceed the total rewards as a break in the route results in no rewards being given to intermediate nodes.

Receipt Based Schemes (RBS): Receipt based schemes are designed to eliminate the need of a TPD and involve

Table 1: Summary of cooperation stimulation strategies

Scheme	Advantage	Limitations
Tamper proof device based schemes	No single point of failure	TPD can be compromised by external attackers due to open communication medium
Receipt based schemes	Protection from external attackers through cryptographically protected proofs	Trusted party or accounting center can be single point of failure

a trusted centralized unit termed as Accounting Center (AC). The intermediate nodes on the route which extend the packet relay service generate payment receipts. These receipts are undeniable proofs of their service which comprise the following, payer identity, payee identity and the payment amount. Protection against forgery is provided cryptographically. A connection with the AC is established periodically, so as to process the receipts which have been accumulated.

RACE (Mahmoud and Shen, 2013) is a lightweight approach based upon incentives, so as to stimulate cooperation of nodes in a multihop ad hoc network. It intends to lower the overhead involved in the process of submission and processing of payment data by the AC. It ensures that no cryptographic operations are needed, since, payment verification can be done through the examination of the consistency of the reports. Each submits reports to the AC which quantify the the packet forwarding activity and the verification is accomplished through undeniable proofs which act as evidences. The role of evidences comes into picture in case of a cheating report, so as to identify and eliminate the nodes which submit forged reports. Table 1 briefs summary of two schemes.

RESULTS AND DISCUSSION

Classification of cooperation enforcement schemes: The strategy employed by these schemes is based upon quantification of behavioral charecteristics of a MANET node. Each node in the MANET performs the neighborhood monitoring with regard to forwarding activity. It involves the metrics related to in-bound and out-band traffic of a neighboring node. Another approach involves sending of acknowledgement packets as a packet reception proof by intermediate node to their upstream neighbors. Yet another approach involves the probing of source to destination path, so as to identify packet droppers. It involves the behavior sampling of a network by sending traffic. The traffic can be either simple probe packets or complex test transactions which facilitate the computation of metrics associated with end-to-end communication points. These metrics include latency, loss and route availability. A classification of cooperation enforcement schemes based upon the behavior monitoring mechanism is as follows:

- Promiscuous Monitoring Schemes (PMS)
- Acknowledgement based Schemes (AMS)
- Probing Based Schemes (PBS)

Promiscuous Monitoring Schemes (PMS): The schemes involve an additional responsibility for all the nodes in the network requiring them to monitor the forwarding behavior of its neighbors through promiscuous listening of neighborhood. In the simplest form nodes maintain counts of incoming packets and outgoing packets at each of their neighbors. Such an approach is based upon a traffic invariant called principle of conservation of flow according to which there exists a direct relation between the incoming traffic and the outgoing traffic at a node. A collaborative monitoring self-organized approach wherein each node is equally responsible for security through localized collaboration and information cross-validation has been proposed by Yang *et al.* (2006). The security solution named as SCAN is based upon the public key cryptography which employs a polynomial secret sharing scheme. Another scheme termed as Secure and Objective Reputation-based Incentive (SORI) scheme performs reputation assessment of a node using objective measures that rely on neighborhood monitoring by having the nodes operate in promiscuous mode to monitor the packet forwarding activity of their neighbors has been proposed.

Acknowledgement Based Schemes (ABS): These schemes require the nodes which perform packet forwarding to send acknowledgements to their on-path upstream nodes in the direction that is the reverse of data transmission. An acknowledgement based scheme is the 2ACK technique proposed by Kejun (Liu *et al.*, 2007) in which the misbehavior is detected through a special two hop acknowledgement packet termed as 2ACK packet. Its path is fixed to a pre-defined route of two hops in the upstream direction of the data transmission. Misbehavior detection is done by considering the number of data packets with missing 2ACK packets.

An acknowledgement based approach for detecting the packet droppers and isolating them has been proposed (Djenouri and Badache, 2008). It mainly involves two components of monitoring and judgment where in the former employs two-hop ACK scheme and the latter component relies upon Bayesian technique to

Table 2: Summary of cooperation enforcement strategy schemes

Scheme	Advantage	Limitations
PMS	No additional control overhead	More energy consuming and inaccuracies due to collisions
ABS	Inaccuracies in behavioral monitoring are reduced	Control overhead in the form of acknowledgement packets

eliminate the incorrect detections caused due to environmental reasons which include mobility of nodes and channel conditions. An approach based upon the combination of principle of flow of conservation (Gonzalez *et al*., 2008) and the 2-hop ACK is proposed (Samreen and Narsimha, 2013a-c). It performs the identification of a misbehaving node after the detection of a suspicious link to guard the non-malicious node against false accusation.

Probing Based Schemes (PBS): A protocol which employs a probing based approach is the On Demand Byzantine Resilient Routing Protocol (ODBSR) (Awerbuch *et al*., 2008). It counters the colluding byzantine behavior through an adaptive probing technique. The scheme monitors the fault occurrence count and after it reaches log n (where n stands for path length), it initiates the malicious link detection. Another probing based approach which performs misbehavior detection through a resource efficient accountability mechanism is the REAct system (Kozma and Lazos, 2009). It is based upon random audits employing bloom filters, so as to have minimal storage requirements which adds to the feasibility of the scheme to a MANET environment.

A secure hybrid routing protocol to form the routes avoiding the malicious packet droppers working individually or in collusion has been proposed (Samreen and Narsimha, 2013a-c). Detection of adversarial nodes on the source to destination path is done through a mechanism employing node behavioral proofs based upon bloom filters. The security mechanism updates the weight assigned to the adversarial nodes followed by the propagation of the information. It results in the update of the proactive routing tables involving the adversarial node which finally results in the establishment of a route involving intermediate nodes with good behavioral characteristics pertaining to packet relay. Table 2 briefs summary of cooperation enforcement strategy schemes.

CONCLUSION

Cooperation stimulation mechanisms implicitly depend upon either a Tamper Proof Device (TPD) or a trusted central authority. The former utilizes a decentralized approach wherein a TPD may be installed in every node. In an open network like MANET, it is an approach vulnerable to external attackers. The latter approach is a centralized approach wherein cryptographically protected proofs of packet forwarding are sent to the Accounting Center (AC). The level of protection against attackers depends completely upon the AC which can revert the whole security mechanism if compromised.

Promiscuous monitoring approach is energy consuming which is not feasible in a MANET environment with limited battery power. It also results in false alarms caused as a result of receiver collisions and ambiguous collisions. The usage of promiscuous monitoring may not be feasible in multi-channel networks as they involve the usage of directional antennas which are associated with parallel transmissions. Acknowledgement-based approaches are relatively more reliable but have to be designed, so as to minimize the unavoidable additional overhead in the form of acknowledgement packets. Probing based approaches incur relatively lesser overhead compared to acknowledgement based approaches and are based upon the detection of abnormalities in packet forwarding activity.

REFERENCES

Awerbuch, B., R. Curtmola, D. Holmer, C. Nita-Rotaru and H. Rubens, 2008. ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. ACM. Trans. Inf. Syst. Secur., 10: 1-35.

Djenouri, D. and N. Badache, 2008. Struggling against selfishness and black hole attacks in MANETs. Wireless Commun. Mobile Comput., 8: 689-704.

Gonzalez, O.F., G. Ansa, M. Howarth and G. Pavlouk, 2008. Detection and Accusation of packet forwarding misbehavior in mobile ad-hoc networks. J. Internet Eng., 2: 181-192.

Kozma, W. and L. Lazos, 2009. REAct: Resource-efficient accountability for nodemisbehavior in ad hoc networks based on random audits. Proceedings of the 2nd ACM Conference on Wireless Network Security, March 16-19, 2009, ACM, Zurich, Switzerland, ISBN:978-1-60558-460-7, pp: 103-110.

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mobile Comput., 6: 536-550.

Mahmoud, M.M. and X. Shen, 2013. A secure payment scheme with low communication and processing overhead for multihop wireless networks. Parallel Distrib. Syst. IEEE. Trans., 24: 209-224.

Perlman, R., 2000. Interconnections: Bridges, Routers, Switches and Internetworking Protocols. 2nd Edn., Pearson Education, Upper Saddle River, New Jersey, ISBN:81-7758-969-5, Pages: 539.

Pouyan, A. and M.Y. Tabari, 2014. Estimating reliability in mobile ad-hoc networks based on Monte Carlo simulation. Intl. J. Eng. Trans. B Appl., 27: 739-746.

Samreen, S. and G. Narasimha, 2013a. A secure hybrid routing protocol to combat malicious packet dropping in a MANET. Intl. J. Comput. Appl., 65: 29-35.

Samreen, S. and G. Narsimha, 2013b. An efficient security mechanism to detect the packet droppers in a MANET under individual and collusive adversarial models. Intl. J. Comput. Appl., 82: 39-43.

Samreen, S. and G. Narasimha, 2013c. An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour. Proceedings of the 2013 IEEE 3rd International Conference on Advance Computing (IACC'13), February 22-23, 2013, IEEE, Ghaziabad, India, ISBN:978-1-4673-4527-9, pp: 588-592.

Taghizadeh, S.R. and S. Mohammadi, 2013. Lebrp-a lightweight and energy balancing routing protocol for energy-constrained wireless ad hoc networks. Intl. J. Eng. Trans. A Basics, 27: 33-38.

Weyland, A. and T. Braun, 2004. Cooperation and accounting strategy for multi-hop cellular networks. Proceedings of the 13th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN'04), April 28, 2004, IEEE, Mill Valley, California, USA., ISBN:0-7803-8551-9, pp: 193-198.

Weyland, A., T. Staub and T. Braun, 2006. Comparison of motivation-based cooperation mechanisms for hybrid wireless networks. Comput. Commun., 29: 2661-2670.

Yang, H., S.J.X. Meng and S. Lu, 2006. SCAN: Self-organized network-layer security in mobile ad hoc networks. IEEE J. Selected Areas Commun., 24: 261-273.

Zhang, Y., W. Lou, W. Liu and Y. Fang, 2007. A secure incentive protocol for mobile ad hoc networks. Wirel. Netw., 13: 569-582.