International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-2)

Research Article | **February 2017**

Data Exchange in Ad-Hoc Network Using AMD and Two-Step Authentication Framework

Pournima Sadhu, R. C. Roychaudhary
Department of Computer Science & Engineering, St Vincent Pallotti College of Engineering & Technology, Nagpur, Maharashtra, India

Abstract—

Intrusion detection over the last few years, assumed top importance in the world of network security and as in the case of wireless adhoc networks also. These are the networks that do not have an underlying infrastructure, network topology which are constantly changing. Because of increased vulnerabilities, Threats and Illegal Access intrusion prevention alone does not solve the problem. Intrusion detection for wireless adhoc networks is a complex and difficult task mainly due to the dynamic nature, their highly constrained nodes, and the lack of central monitoring points. Intrusion prevention systems are considered as extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.In this paper we present outlines of the issues of intrusion detection and prevention for wireless adhoc networks.

Keywords— Intrusion, AMD, Authentication, AdHoc

I. INTRODUCTION

We address the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks. We develop a comprehensive system called Audit-based Misbehavior Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. Compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes.

Wireless Sensor Networks (WSNs) can be used in a broad range of applications from complex military operations to simple domestic environments. This makes security a vital characteristic in WSNs. There have been numerous studies in the field of security in sensor networks, being Intrusion Detection System (IDS) among the most used tools in this area. This study proposes a new IDS design based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks.

Mobile Ad hoc networks (MANETs) are susceptible to having their effective operation compromised by a variety of security attacks because of the features like unreliability of wireless links between nodes, constantly changing topology, restricted battery power, lack of centralized control and others. Nodes may misbehave either because they are malicious and deliberately wish to disrupt the network, or because they are selfish and wish to conserve their own limited resources such as power. In this paper, we present a mechanism that enables the detection of nodes that exhibit packet forwarding misbehavior. The approach is based on the usage of two techniques which will be used in parallel in such a way that the results generated by one of them are further processed by the other to finally generate the list of misbehaving nodes. The first part detects the misbehaving links using the 2ACK technique and this information is fed into the second part which uses the principle of conservation of flow (PFC) technique to detect the misbehaving node.

AMD is a comprehensive solution that integrates identification of misbehaving nodes, reputation management, and trustworthy route discovery in a distributed and resource-efficient manner.

We develop the AMD system for detecting and isolating misbehaving nodes. Compared to state-of-the-art, AMD provides the following additional features:

- AMD enables the per-packet evaluation of a node's behavior without incurring a per-packet overhead.
- AMD enables the concurrent first-hand evaluation of the behavior of several nodes that are not necessarily one-hop neighbors. Overhearing techniques are limited to one hop.
- AMD can operate in multi-channel networks and in networks with directional antennas. Current packet overhearing techniques are only applicable when transmissions can be overhead by peers operating on the same frequency band.
- AMD detects selective dropping behaviors by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when endto- end traffic is encrypted. In the latter scenario, only the source and destination have access to the contents of the packets and can detect selective dropping.

We will used Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes, which relies on two modules, the watchdog and the pathrater. The watchdog module is responsible for overhearing the transmission of a successor node, thus verifying the successful packet forwarding to the next hop. The pathrater module uses the accusations generated by the watchdog module to select paths free of misbehaving nodes.

Also we add a scheme which efficiently detects the misbehaving nodes so that they may be discarded from the network. It is based on the usage of two techniques: 2ACK scheme and PFC (Principle of Flow of Conservation) scheme.

II. LITERATURE SURVEY

1) Misbehaving router detection in link-state routing for wireless mesh networks

Author: Ács, G. Lab. of Cryptography & Syst. Security (CrySyS), Budapest Univ. of Technol. & Econ., Budapest, Hungary

Description: In this paper, they address the problem of detecting misbehaving routers in wireless mesh networks and avoiding them when selecting routes. We assume that link-state routing is used, and we essentially propose a reputation system, where trusted gateway nodes compute Node Trust Values for the routers, which are fed back into the system and used in the route selection procedure.

The results show that our proposed mechanism can detect misbehaving routers reliably, and thanks to the feedback and the exclusion of the accused nodes from the route selection, we can decrease the number of packets dropped due to router misbehavior considerably. At the same time, our mechanism only slightly increases the average route length.

2) ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks

Author: B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens

Description: Ah hoc networks offer increased coverage by using multihop communication. This architecture makes services more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. In this work, they examine the impact of several Byzantine attacks performed by individual or colluding attackers. We propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes.

Paper demonstrate through simulations ODSBR's effectiveness in mitigating Byzantine attacks Paper analysis of the impact of these attacks versus the adversary's effort gives insights into their relative strengths, their interaction, and their importance when designing multihop wireless routing protocols.

3) Reputation-based Intrusion Detection System for wireless sensor networks

Author: Keldor Gerrigagoitia, Roberto Uribeetxeberriay, Urko Zurutuzaz, and Ignacio Arenaza

Description : In this work they review the work done so far on Intrusion Detection Systems for WSN, then we focus on reputation and trust based systems, and finally we propose a new architecture based on the most suitable features of the reviewed systems that can lead to a complete and industrially usable IDS for WSN. Here some IDS are proposed where special purpose nodes in the network which are responsible for monitoring other nodes.

They listen to messages in their same radio range and store message fields that can be useful to an IDS running in a sensor node. There are some other different points of view in the design of IDS in WSN, for example , where nodes are selfish and try to preserve their resources at expense of others. Other works keep the idea of no collaboration among sensor nodes and assume that the ad hoc network routing protocols can be applied to WSN.

4) Preventing Selfishness in Open Mobile Ad Hoc Networks

Author: H. Miranda and L. Rodrigues,

Description: A particular characteristic of ad hoc networks is their self-organization, what makes them highly dependable of the participants. This position paper shows how the selfishness of the participants in a ad hoc network can prejudice its overall functioning and sketches a protocol that discourages this kind of behavior . As previously mentioned, MANETs where envisioned for search-and-rescue, military and law enforcement operations. In these examples, all users work together toward a common goal. There- fore, selfishness behavior is not expected since it would only prejudice the group. We envision that MANETs will rapidly expand to other domains, like the one presented above. In these Open

MANETs, users do not share a common goal. Each user will agree to share his resources only if this brings him some benefit and not to the group as in Closed MANETs

III. PROPOSED METHODOLGY

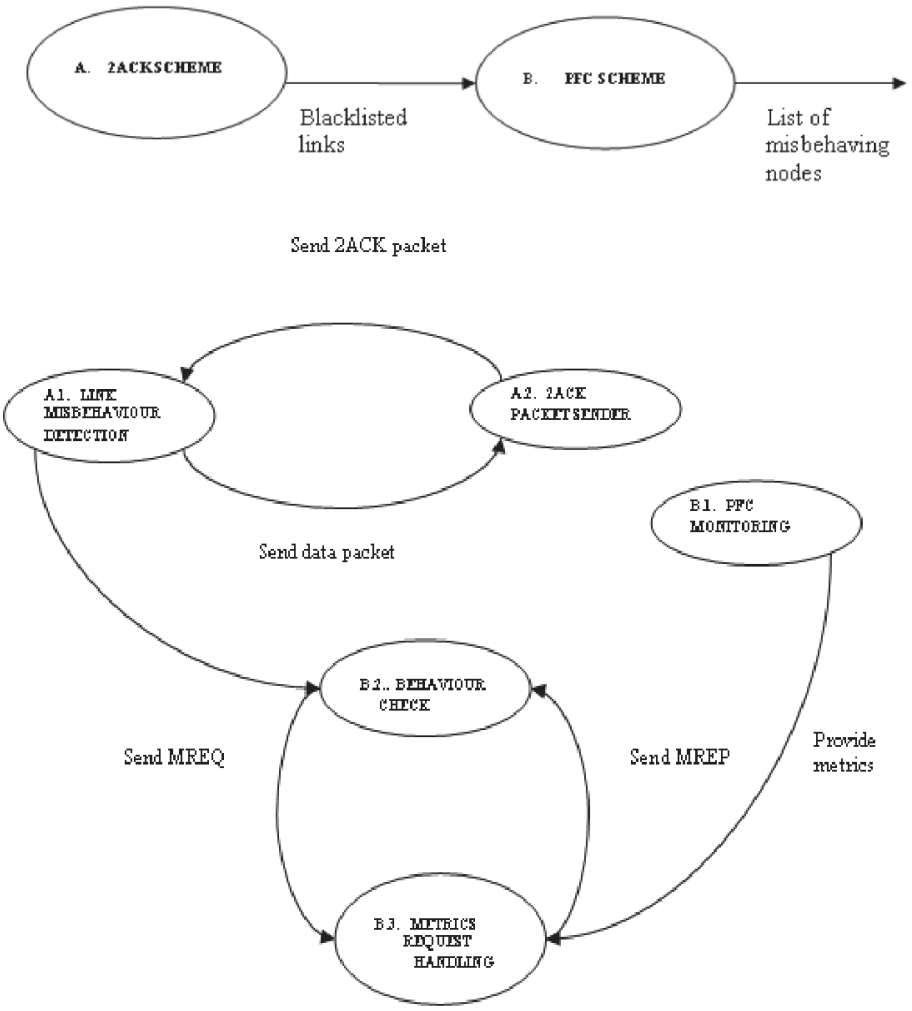
Here we proposed two technique in methodology

An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour

The approach is based on the usage of two techniques which will be used in parallel in such a way that the results generated by one of them are further processed by the other to finally generate the list of misbehaving nodes. The first part detects the misbehaving links using the 2ACK technique and this information is fed into the second part which uses the principle of conservation of flow (PFC) technique to detect the misbehaving node. The problem with the 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving. Hence we use the principle of conservation of flow, PFC for the second part which detects the misbehaving nodes associated with that of the misbehaving link

Each node keeps running the 2ACK algorithm whenever a route has to be established from a source node S to a destination node D. The 2ACK technique involves the logical formation of overlapping triplets upon the routing path from source S to destination D. The module LINK MISBEHAVIOUR DETECTION is executed by a node which is logically the first one in a triplet along the route. It forwards / sends the data packet and applies the concept of 2ACK technique to determine the misbehaving link. The module 2ACK PACKET SENDER is executed by a node which is logically the last one in the triplet along a route. It receives the data packet and as per the 2ACK technique, if it is well behaving then, it is supposed to send 2ACK packet over two hops in the reverse direction to that node which is the first one in the triplet. Once a link is blacklisted, each of the nodes checks to see if any of their neighbors are associated with this link. The module BEHAVIOUR CHECK performs this task.

It gathers the metrics associated with the neighbor node by broadcasting MREQ packets which stand for metrics request packet. It then sets a timer and starts waiting for MREP (metrics reply) packets from each of the associated neighboring nodes which are all accumulated. Once all MREP packets are received, it checks to see if PFC condition is satisfied to arrive at a conclusion of whether the node being checked is well behaving or misbehaving. The sending of MREQ packets by BEHAVIOUR CHECK module invokes another module calledas METRICS REQUEST HANDLING.

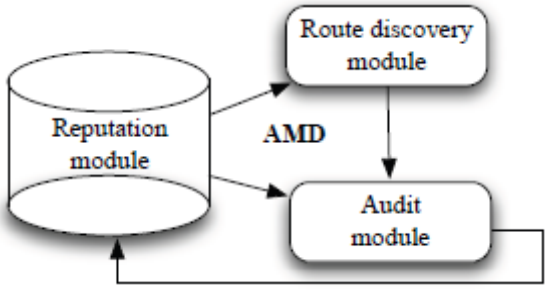


AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks

The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. Compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes. Moreover, AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas. We show via simulations that AMD successfully avoids misbehaving nodes, even when a large portion of the network refuses to forward packets.

AMD provides a comprehensive misbehavior identification and node isolation system for eliminating misbehavior from a given network. This system consists of the integration of three modules:a reputation module, a route discovery module, and an audit module.

These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers. A schematic of the relationship between the three modules of AMD is shown in Figure below. The reputation module is responsible for managing reputation information based on the recommendations of the audit module.



Flow Diagram AMD

Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations. AMD isolates misbehaving nodes by implementing a reputation based system. Nodes with low reputation values are excluded from routing paths, thus being unable to drop transit traffic. The reputation module is responsible for computing and managing the reputation of nodes. We adopt a decentralized approach in which each node maintains its own view of the reputation of other nodes.

Such implementation alleviates the communication overhead for transmitting information to a centralized location, and readily translates to the distributed nature of ad hoc networks. Moreover, it allows nodes to hold individualized reputation metrics for their peers depending on their direct and indirect interactions.

IV. CONCLUSION

We developed AMD, a comprehensive misbehavior detection and mitigation system which integrates three critical functions: reputation management, route discovery, and identification of misbehaving nodes via behavioral audits. We modeled the process of identifying misbehaving nodes as R´enyi-Ulam games and derived resource-efficient identification strategies. We showed that AMD recovers the network operation even if a large fraction of nodes is misbehaving at a significantly lower communication cost.

Moreover AMD can detect selective dropping attacks over endto-end encrypted traffic streams. The proposed scheme efficiently performs the detection of misbehaving node by the combination of 2ACK and the PFC techniques. Since the 2ACK technique detects the misbehaving link but cannot decide which one of the two associated nodes are misbehaving, we extend the technique by applying PFC monitoring as the next step to detect the misbehaving nodes once the misbehaving link is detected. The computational overhead as compared to the original PFC technique is reduced considerably since we are examining only those nodes behavior which are associated with misbehaving links.

REFERENCES

[1] G. Acs, L. Buttyan, and L. Dora. Misbehaving router detection in link-state routing for wireless mesh networks. In Proc. of WoWMoM, pages 1–6, 2010.

[2] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008.

[3] K. Balakrishnan, J. Deng, and P. K. Varshney. Twoack: Preventing selfishness in mobile ad hoc networks. In Proc. of WCNC, 2005.

[4] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. Communications of the ACM, 13(7):422–426, 1970.

[5] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, 2002.

[6] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks," http://secowinet.epfl.ch/, 2006.

[7] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet draft, Feb. 2002.

[8] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan "An acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANETs", IEEE Transactions on Mobile Computing, vol. 6, No. 5, 2007.

[9] Gonzalez et al.: Detection and Accusation of packet forwarding misbehavior in mobile ad-hoc networks, Journal of Internet Engineering, vol. 2, pp.1, 2008.

[10] L. M. Feeney and M. Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In Proc. of INFOCOM, pages 1548–1557, 2001.

[11] S. Ganeriwal, L. Balzano, and M. Srivastava. Reputation-based framework for high integrity sensor networks. ACM Transctions on Sensor Networks, 4(3):1–37, 2008.

[12] K. Hansen, T. Larsen, and K. Olsen. On the efficiency of fast rsa variants in modern mobile phones. Arxiv preprint arXiv:1001.2249, 2010.

[13] Q. He, D. Wu, and P. Khosla. SORI: A secure and objective reputation-based incentive scheme for ad hoc networks. In Proc. of WCNC, 2004.

[14] D. Johnson, D. Maltz, and Y.-C. Hu. The dynamic source routing protocol for mobile ad hoc networks (DSR). draft-ietf-manet-dsr-09.txt, 2003.

[15] A. Jøsang and R. Ismail. The beta reputation system. In Proc. of the 15th Bled Electronic Commerce Conference, pages 324–337, 2002.
[16] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3):293–315, 2003.
[17] W. Kozma and L. Lazos. Dealing with liars: Misbehavior identification via R´enyi-Ulam games. Security and Privacy in Communication Networks, pages 207–227, 2009.
[18] W. Kozma Jr. and L. Lazos. REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. In Proc. Of WiSec, 2009.
[19] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgment based approach for the detection of routing misbehavior in manets. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.
[20] Y. Liu and Y. R. Yang. Reputation propagation and agreement in mobile ad-hoc networks. In Proc. of IEEE WCNC, pages 1510–1515, 2003.
[21] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proc. of MobiCom, pages 255–265, 2000.
[22] P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proc. of CMS, pages 107–121, 2002.
[23] V.-N. Padmanabhan and D.-R. Simon. Secure trace route to detect faulty or malicious routing. SIGCOMM CCR, 33(1), 2003.
[24] A. Pelc. Detecting errors in searching games. Journal of Combinatorial Theory Series A, 51(1):43–54, 1989...

