International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

A Trust-Based Security Scheme for Malicious Node Isolation Based on the Fine-Grained Analysis of Packet Losses

Shaik Shamaheena & S G Nawaz Hod

[1] *M.Tech Student, Dept of CSE, SKD Engineering College, Affiliated to JNTUA, AP, India*

[2] *Associate Professor & HOD, Dept of CSE, SKD Engineering College, Affiliated to JNTUA, AP, India*

ABSTRACT:

In a wireless sensor network, packet losses can result from attacks affecting the nodes or the wireless links connecting the nodes. Failure to identify the actual attack can undermine the efficacy of the attack responses. We need approaches to correctly identify the cause of packet losses Packet losses in a wireless sensor network represent an indicator of possible attacks to the network. Detecting and reacting to such losses is important to determine the actual cause of the loss. In this paper, a scheme is proposed which is able to identify malicious nodes properly using network parameters to determine whether packet losses are due to queue overflows or node mobility in MANETs. The proposed system also includes a fine-grained analysis (FGA) scheme for packet loss and the development of a comprehensive trust model for malicious node identification and separation. Our proposed FGA scheme is evaluated in terms of effectiveness and performance metrics under different network parameters and configurations. The experimental results show that our proposed trust model achieves a significant reduction

Keywords: Mobile security, webpages, web browsers, machine learning.

I. INTRODUCTION

When dealing with wireless sensor networks (WSNs), a class of events that is relevant for SA is represented by packet losses. Such events may lead to the loss of relevant information and may undermine data quality solutions based on redundant transmission of data. As WSNs have been deployed for disaster recovery, tactical missions, and patient monitoring, the sensitivity of these applications leave no room for any data errors. However, in order to achieve full SA, it is not sufficient to detect that packets have been lost. It is also crucial to obtain correct diagnoses about the causes of the losses, as packet losses could be due to misbehaving or compromised nodes or to attacks on the links. For sensor systems to survive, this knowledge is crucial for responding to the attacks and for recovery and debugging purposes. Current intrusion detection systems are typically only able of detecting packet losses and are thus unable to determine the cause of the losses, whether it is node or link related. Attacks like selective forwarding and blackhole attacks are examples of node related attacks that result in partial or total packet losses, while interference is an example of a link related attack. Current intrusion detection techniques thus need to be extended with approaches able to perform a correct diagnosis of the cause of packet losses in the WSN of interest. Without a fine-grained analysis of packet losses in the trust building process, traditional schemes may result in erroneous trust estimations, especially under high data rate and high node mobility. In this paper, we propose a fine-grained analysis (FGA) scheme that investigates the causes of data packet losses and reports the most likely cause of these losses. We first identify the key parameters for analyzing the cause of packet losses under different aspects.

II. LITERATURE SURVEY

1) E. M. Shakshuki, N. Kang, and T. R. Sheltami, Eaack— a secure intrusion-detection system for MANETs,.

The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

2) Y. Lu, Y. Zhong, and B. Bhargava, Packet loss in mobile ad-hoc.

We investigate packet loss in mobile ad hoc networks via simulation. Ad-hoc on-demand distance vector (AODV) and destination-sequenced distance vector (DSDV) are chosen as representatives of the on-demand and proactive routing protocols respectively. The effects of congestion and mobility in various network contexts are explored. The results indicate that DSDV loses 10% to 20% more packets than AODV does for UDP traffic. For TCP traffic, the packet loss for DSDV is a half of that for AODV. Mobility is the dominant cause for AODV, which is responsible for more than 60% of total packet loss. For DSDV, more than 50% of total packet loss is congestion related. Sample data shows that the packet loss distribution over time is bursting, which makes the tradition Poisson framework unsuitable for modelling it. Preliminary results exhibit self-similar pattern that leads us to believe that fractal model is promising to describe packet loss in ad hoc networks. This work provides guidelines for the design of routing and flow control algorithms and insights in choosing proper parameters in future simulation and analytic studies.

3) Z. Chen, Z. Ge, and M. Zhao, A load-based queue scheduling algorithm for MANET.

In the mobile ad hoc networks, due to the multi-hop of the data, the limited bandwidth and the dynamic changes of the network topology, the network performance is hindered. This paper proposes a Load-based Queue Scheduling algorithm (LBQS) for MANET. Nodes thoroughly consider their own load states when forwarding packets. The priorities of packets are assigned according to the current node's load level. When nodes are leisure, they should help other nodes to construct route first. In order to avoid network transmission delay increasing and packets losing, nodes should delay or forbid the construction of new route passing through them when their load level is high. The simulation results show that LBQS algorithm can effectively decrease the network transmission delay and promote the network throughput to a certain extent.

4) Dynamic Source Routing in *ad hoc* wireless networks.

An advert hoc community machine is an accumulation of far off flexible hosts framing a transitory device without the manual of any incorporated agency and installation framework. In

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

this type of conditions, it might be vital for each transportable hub host to enroll the suggest of exchange hosts in sending parcel from supply to vacation spot. Because of its constrained scope of each flexible hub host's remote transmissions. This paper exhibits a DSR Protocol (detail source directing convention) for Ad-hoc structures. This conference adjusts directing changes right away when flexible hub moves starting with one location then onto the following yet it requires a nearly no overhead amid durations in which transportable hubs actions progressively. In view of the effects from a bundle degree reenactment of portable hubs running in a especially appointed device, the DSR conference performs notably well in an change ecological conditions, for example, improvement fees and host thickness. For everything besides the most increased quotes of developments in hosts is mimicked, the overhead of the conference is absolutely low, tumbling to best 1% of aggregate statistics bundles transmitted for moderate development fees in a device of 24 transportable hosts.

III. EXISTING METHOD:

- Anjum et al. proposed a lightweight packet drop detection for ad-hoc networks (LiPaD). They suggested that every node must keep a count of received/forwarded packets and periodically report to a coordinator node for analysis and malicious node detection. Such technique requires a computationally powerful, central coordinator node that is practically not feasible in MANETs.
- Another system which is collaborative reputation-based solution, called CORE, was proposed by Michiardi et al. to evaluate the reputation of a node. They suggested that collaborative reputation is the combination of subjective, indirect, and functional reputations. A reputation table is maintained at each node to record the reputation of other nodes and to determine whether a node is malicious or not.

DISADVANTAGES OF EXISTING SYSTEM:

- Considered each packet loss as misbehavior by malicious nodes, without analyzing the other possible causes of packet losses.
- High false positive rate.
- Consume more energy.

IV. PROPOSED METHOD:

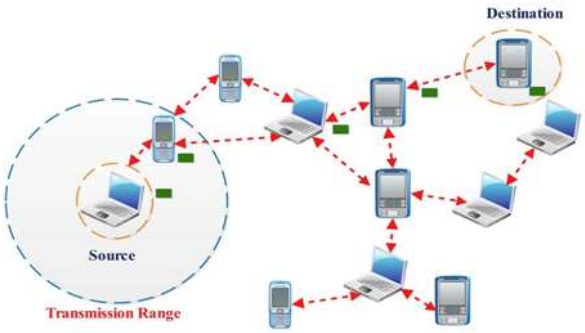
- We propose a fine-grained analysis (FGA) scheme that investigates the causes of data packet losses and reports the most likely cause of these losses. We first identify the key parameters for analyzing the cause of packet losses under different aspects.
- Our FGA scheme uses several different parameters such as MAC layer information, queue information, and rate of link changes to profile the links between nodes as well as the nodes' neighborhoods. The reason for using local information at each node is to achieve more accurate information and view of network.
- Although global information may in some cases provide sufficient information, it is possible that false information provided by the misbehaving node can circumvent the security mechanisms. Moreover, as the FGA scheme requires information about the node neighborhood, each node uses its own local information to take a more in-formed decision.

ADVANTAGES OF PROPOSED METHOD:

- High and accurate detection rate.
- Low false positive rate.
- Consider and analyze cause of packet loss.

SYSTEM ARCHITECTURE

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018



V. MODULES

ACK implementation:

ACK is an end-to-end acknowledgment scheme acts as a part of the hybrid scheme in the proposed work aiming to reduce the network overhead when no network misbehavior is detected.

The working of ACK hybrid scheme can be best illustrated from the above figure explained as below:

1. ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D.
2. If all the intermediate nodes along the route between the nodes S and D are successfully cooperative and if node D successfully receives *Pad*1, node D then sends back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order.
3. If within a predefined time span, if node S receives *Pak*1, then the packet transmission from node S to node D is successful. Else, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the transmitted route.

Secure Acknowledgment (S-ACK):

The S-ACK scheme proposed by Liu *et al.* is an improved version of the TWOACK scheme to let every three consecutive nodes work in a group to detect misbehaving nodes. The S-ACK mode is intended to detect misbehaving nodes in the presence of collision or limited transmission power. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node.

In S-ACK mode, assuming the three consecutive nodes as F1, F2, and F3 works in a group to detect misbehaving nodes in the network.

1. At the sender part node F1 first sends out S-ACK data packet *Psad*1 to node F2. Further, node F2 forwards this packet to node F3.
2. At the receiver side when node F3 receives *Psad*1, the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 further forwards *Psak*1 back to node F1.
3. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious and a misbehavior report will be generated by node F1 and sent to the source node S.

Fine Grained Analysis (FGA):

The **FGA** scheme is intended to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. This false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. With this attack the attackers can break down sufficient nodes and thus cause a network division. The crucial part of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

The functionality of the **FGA** mode can be better explained as below:

1. As the initial step, the source node first searches itslocal knowledge base and seeks for an alternative route to the destination node.
2. If no route exists, the source node starts a DSR routing request to find another alternative route. By searching for an alternative route to the destination node, when the destination node receives an **FGA** packet, the source node searches its local knowledge base and compares if the reported packet has been received.
3. If it has already received the packet , then it is safe to conclude that the generated misbehavior

report in S-ACK is a false misbehavior report and the node whoever has generated this report is marked as malicious node. Else, the misbehavior report is trusted and accepted.

Digital Signature Validation:

All three parts ACK, S-ACK, and FGA, are acknowledgment-based detection schemes. All of these schemes rely on acknowledgment packets to detect misbehaviors in the network. Hence, it is extremely important to ensure that all acknowledgment packets are authentic and untainted. If the intruders are smart enough to forge the acknowledgment packets, then all of the above said three schemes are made vulnerable.

To ensure the integrity, it is required that requires all acknowledgment packets to be digitally signed before they are sent out at the source node and verified until they are accepted at the destination.

VI. CONCLUSION

In this paper, a scheme is implemented which is able to identify malicious nodes properly using network parameters to determine whether packet losses are due to queue overflows or node mobility in MANETs. The proposed system also includes a fine-grained analysis (FGA) scheme for packet loss and the development of a comprehensive trust model for malicious node identification and separation. The proposed FGA scheme is evaluated in terms of effectiveness and performance metrics under different network parameters and configurations. The experimental results show that our proposed trust model achieves a significant reduction.

REFERENCES

[1] Villas L.A, Boukerche A, Ramos H.S, De and Loureiro A.A.F (2013)"DRINA:A Lightweight Aggregation in Wireless Sensor Networks," IEEETrans.,on computers, vol.62 No.4, pp 676-689.,2013

[2] Al-Karaki J, Ul-Mustafa R, and Kamal A , "Data Aggregation in Wireless Sensor Networks — Exact and Approximate Algorithms,"Proc. High Performance Switching and Routing Workshop (HPSR '04),pp. 241-245,2004.

[3] Akyildiz I.F, Su W, Sankarasubramaniam Y, and Cyirci E, "Wireless Sensor Networks: A Survey," Computer Networks, vol.38, no. 4, pp. 393-422,2002.

[4] Anastasi G, Conti M, Francesco M, and Passarella A , "Energy Conservation in Wireless Sensor Networks: A Survey," Ad Hoc Networks, vol.7,no. 3, pp. 537- 568,2009. http://dx.doi.org/10.1016/j.adhoc.2008.06.003.

[5] Chandrakasan A.P, Smith A.C, and Heinzelman W.B , "An Application-Specific Protocol Architecture for Wireless Microsensor Networks,"IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670,2002.

[6] Krishnamachari B, Estrin D, and Wicker S.B, "The Impact of Data Aggregation in Wireless Sensor Networks," Proc. 22nd Int'l Conf. Distributed Computing Systems (ICDCSW '02), pp. 575-578,2005

[7] Nakamura E.F, Loureiro A.A.F, and Frery A.C "Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications," ACM Computing Surveys, vol. 39, no. 3, pp. 9-1/9-55,2007

[8] Romer K and Mattern F, "The Design Space of Wireless Sensor Networks,"IEEE Wireless Comm., vol. 11, no. 6, pp. 54-61,2004.

[9] Villas L.A, Boukerche A, Araujo R.B, and Loureiro A.A (2009), "A Reliable and ACM Int'l Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 245-252,

[10] Younis O, Krunz M, and Ramasubramanina S, "Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges," IEEE Network, vol. 20, no. 3, pp. 20-25,2006.