ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

DETECTION OF MISBEHAVING PACKET DROPPERS AND MODIFIERS IN WIRELESS NETWORKS USING AN ADAPTIVE PROTOCOL

Sudha.L[1], Muthukumarasamy.S[2]

PG Scholar, Dept. of CSE, S.A Engineering College, Chennai, Tamil Nadu, India[1]

Assistant Professor, Dept. of CSE, S.A Engineering College, Chennai, Tamil Nadu, India[2]

ABSTRACT: **Security is one of the most challenging issues in the field of communication networks. Denial-of-service (DoS) attacks on wireless networks (WNs) can deplete network resources and energy without much effort on the part of an adversary. Packet dropping attacks are one category of DoS attacks. In a wireless networks packet dropping and modification are more common attacks that can be launched by an attacker to disrupt communication. Current techniques for detecting such attacks need to monitor every node in the network. Once they detect malicious nodes that drop packets, a new path has to be found that does not include them. In this paper, we propose a scheme, which can identify misbehaving forwarders that drop or modify packets in the wireless networks. DAV protocol is implemented to detect misbehaving node to drop packets. An adaptive mechanism is developed to encrypt packet from packet modifiers. The goal is to mitigate packet dropper and modifier in wireless networks**.

Keywords- Denial-of-service, Wireless networks, Packet dropping, packet modification.

I. INTRODUCTION

WIRELESS networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, packet drooping and modifying attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. After compromising one or multiple nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward. A compromised node can launch the following two attacks:

Packet dropping: A compromised node drops all or some of the packets that is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as framing innocent nodes.

Packet modification: A compromised node modifies all or some of the packets that is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes.

To deal with packet droppers, a widely adopted countermeasure is multipath forwarding, in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught.

II. EXISTING SYSTEM

Existing schemes to detect packet dropping attacks can be categorized as three classes: forwarding packets in multipath, monitoring the neighbor nodes, and acknowledgment based detection. Multipath forwarding is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths. The watchdog method was originally proposed to mitigate routing misbehavior in mobile ad hoc networks. It is then adopted to identify packet droppers in wireless network. When the watchdog mechanism is deployed, each node monitors its neighborhood promiscuously to collect the firsthand information on its neighbor nodes. A variety of reputation systems have been designed by exchanging each node's firsthand observations,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

which are further used to quantify node's reputation. Based on the monitoring mechanism, the intrusion detection systems are proposed. The third approach to deal with packet dropping attack is the multi hop acknowledgment technique. By obtaining responses from intermediate nodes, alarms, and detection of selective forwarding attacks can be conducted. To deal with packet modifiers, most of existing countermeasures are to filter modified messages within a certain number of hops so that energy will not be wasted to transmit modified messages. Ye et al. proposed a probabilistic nested marking (PNM) scheme. But with the PNM scheme, modified packets should not be filtered out en route because they should be used as evidence to infer packet modifiers. Hence, it cannot be used together with existing packet filtering schemes.

A. ISSUES INVOLVED IN EXISTING SYSTEM

- High-energy cost.
- Storage overhead
- Bidirectional communication links, it may not be effective when directional antennas are used

III. PROPOSED SYSTEM

Proposed system dealt to detect packet droppers and packet modifiers in wireless networks. our basic approach for misbehavior detection, a node (sender) which needs to send data to other node (receiver) via intermediate nodes. Though our network is wireless intermediate nodes are chosen dynamically where packets can be transmitted. A trust node is designed to be a part of communication in network. It designed the route where packet is transmitted. To detect misbehaving node in the network, it executes a DAV protocol to generate a secret value which is added in the packet. Once an intermediate which receives a packet, it needs to send packet to other node and it reports to trust with that secret value. A secret value can be generated for each intermediate node randomly and it should be allocated by trust node. To mitigate packet modifiers we introduce a cryptographic CPT schemes to hide the packet which cannot modify by an adversary.

B. FEATURES OF PROPOSED SYSTEM

1) Being effective in identifying both packet droppers and modifiers,
2) Low communication and energy overheads, and
3) being compatible with existing false packet filtering schemes; that is, it can be deployed together with the false packet filtering schemes, and therefore it cannot only identify intruders but also filter modified packets immediately after the modification is detected.

IV. SYSTEM ARCHITECTURE

The source node sends data packet to the destination node through the intermediate nodes. The intermediate node misbehaves by dropping packets and act as packet droppers. The trust node generates a secret value that attached with each packet to other nodes. The nodes which received a packet are sent to other node and verify a secret value with trust node. The trust node didn't get ack from nodes, it detects that node has dropped packets. The trust node plays a vital role here in detecting the misbehaving node. Destination node on receiving the data sends the trust node an ack to intimate the receipt of data. Fig 1 represents system architecture to detect misbehaving packet droppers.

To mitigate packet modifiers proposed scheme introduced a mechanism to encrypt packet from node to node transmission.Fig.2 shows System architecture to prevent misbehaving packet modifiers.

V. THE ADAPTIVE PROTOCOL

The Dynamic Allocation Value (DAV) protocol is effective, DoS- resistant protocol in which Packet dropper can be identified. The key idea of the protocol is a node which needs to send a packet that executes a protocol in wireless network.a trust node can choose randomly and it generates a secret value that can be added with packet.a node which receives packet that executes DAV protocol and verifies wuth trust node.

Under the DAV protocol, the nodes and trust node behave as follows:

DAV PROTOCOL in intermediate nodes:

- Receive packet
- Executes DAV
- Send ack with secret value

DAV PROTOCOL in Trust node:

- Establish route.
- Executes DAV
- Checking misbehaving node
- Backlist node

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

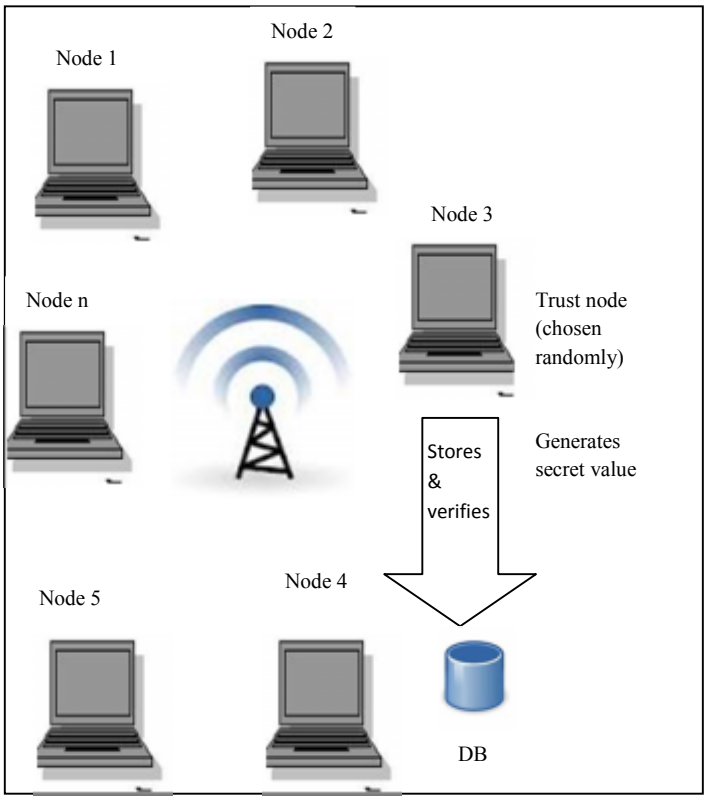

Fig.1 System architecture to detect misbehaving packet droppers.

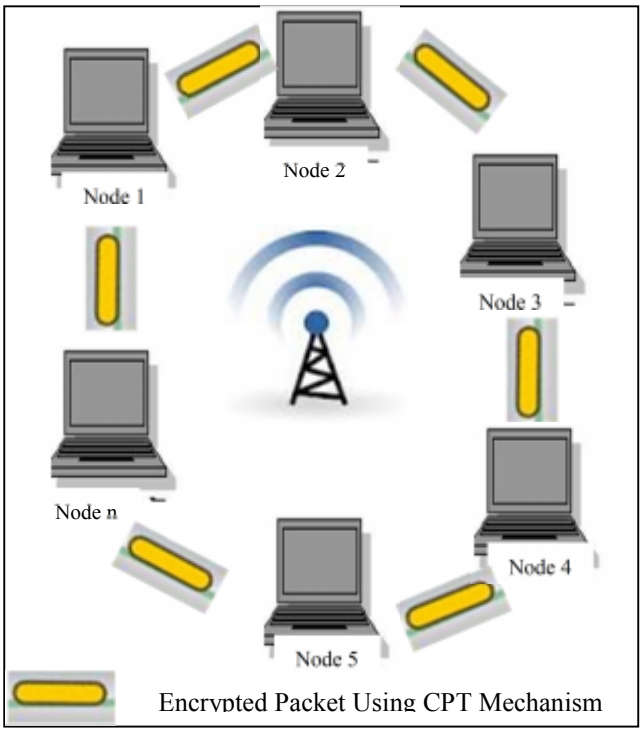

Fig.2 System architecture to prevent misbehaving packet modifiers.

VI. WORKING OF THE SYSTYEM

C. IDENTIFICATION OF NODES

Identify the nodes which needs to packet transmission in the network. The nodes in the network do not have interaction before transmission. Once the connection is established, nodes contacts and establish communication to transfer packets.

D. CHOOSING OF TRUST NODE

In wireless network, choose trust node is important for packet transmission in order to mitigate packet droppers. Randomly choose trust node by a sender node which needs to send data to receiving node.

E. PROTOCOL IMPLEMENTATION

A trust will monitor the intermediate node which avoids packet droppers in wireless network. It generates secret value to each intermediate with the packet. Once the packet received by intermediate node, it needs to send the packet to other intermediate node and should verify the secret value with trust node.

F. PROTOCOL IMPLEMENTATION

A trust will monitor the intermediate node which avoids packet droppers in wireless network. It generates secret value to each intermediate with the packet. Once the packet received by intermediate node, it needs to send the packet to other intermediate node and should verify the secret value with trust node.

G. DETECTING MISBEHAVING NODE

A secret value will not match with the trust node, it seems that the corresponding intermediate node suspect to packet dropper in the wireless network.

H. IMPLEMENTATION OF CPT MECHANISM

To mitigate packet modifiers introduced three cryptographic schemes: 1.Commitment based mitigatiom,2.solving cryptographic puzzles and 3.All-Or-Nothing Transformations.fig 3 shows the implementation of CPT mechanism

1) COMMITMENT BASED MITIGATION:

Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V while keeping m hidden.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

2) SOLVING CRYPTOGRAPHIC PUZZLE:

The main idea behind such puzzles is to force the recipient of a puzzle execute a predefined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. In our context, we use cryptographic puzzles to temporary hide transmitted packets. A packet m is encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of packet modifiers.

3) ALL-OR-NOTHING-TRANSFORMATIONS:

An AONT serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm.

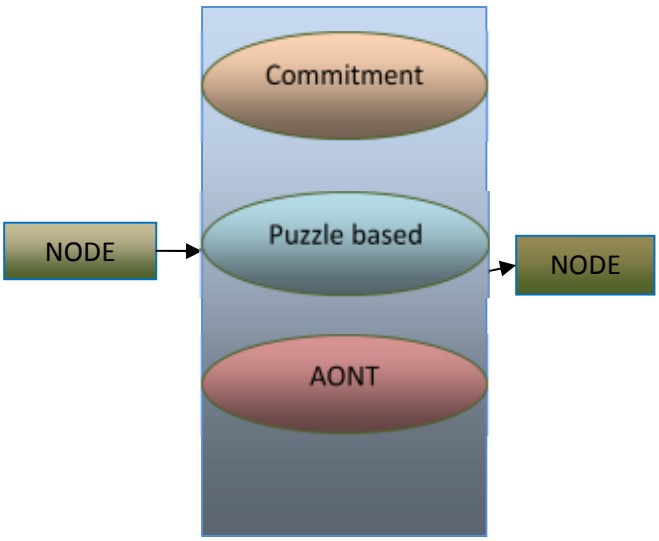

Fig. 3 implementation of CPT mechanism

VII. CONCLUSION AND FUTURE ENHANCEMENT

We propose a simple yet effective scheme to identify misbehaving forwarders that drop or modify packets in wireless networks. Each packet is encrypted and padded so as to hide the source of the packet. A small number of extra bits as secret value can be added to detect packet droppers. Moreover, the nodes encrypt a packets using CPT mechanism to mitigate from packet modifiers. The proposed is very generic it does not rely on any routing algorithms. Extensive analysis, simulations, and implementation have been conducted and verified the effectiveness of the proposed scheme.

The further enhancement can be done by providing more security to provide alarm to each intermediate node instead of generating secret value randomly. This avoids a node is being compromised by malicious node being detected.

ACKNOWLEDGEMENT

I would like to express my gratitude to all those who gave me the possibility this paper. First, I thank my coordinator and internal guide Mr. Muthukumaraswamy M.E, Department of PG Studies in engineering, without his guidance, this would not be possible. I also wish to record my thanks to our Head of the Department Mrs.Umarani Srikanth M.E (PhD) for her consistent encouragement and ideas.

REFERENCES

[1]H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.
[3] V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005.

[4] M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, "Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

[5] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

[6] R. Rivest, A. Shamir, and D. Wagner, 1996 "Time-Lock Puzzles and Timed-Release Crypto,".

[7] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), 2005.

[8] D. Stinson, 2001 "Something about All or Nothing (Transforms),".

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, 2000.

[10] S. Lee and Y. Choi, "A Resilient Packet-Forwarding Scheme Against Maliciously Packet-Dropping Nodes in Sensor Networks," Proc. Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

[11] I. Krontiris, T. Giannetsos, and T. Dimitriou, "LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

[12] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation- Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.
[13] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management
Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM '10), 2010.
[14] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc
Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security: Advanced Comm. and Multimedia Security, 2002.
[15] T.H. Hai and E.N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge,"
Proc. IEEE Seventh Int'l Symp. Network Computing and Applications (NCA '08), 2008.
[16] F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.
[17] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor
Networks," Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008.
[18] J.M. Mccune, E. Shi, A. Perrig, and M.K. Reiter, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," Proc.
IEEE Symp. Security and Policy, 2005.
[19] A. Juels and J. Brainard, 1999 "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks,".
[20] R. Rivest, 1997 "All-or-Nothing Encryption and the Package Transform,".

Sudha.L received the Bachelor's degree in IT from Anna university Chennai in 2008. She is currently doing Master degree in CSE from Anna university Chennai. Her research interests include data structure, operating system, cryptography, databases, network security and wireless networks.

Muthukumarasamy.S received the B.E degree in computer science and engineering from Anna university Chennai in 2005 and M.E degree in CSE from Anna university Chennai in 2011. His research interest include reliability/security of software systems (include network and mobile system) and program analysis/verification and computer architecture and design, adhoc networks, data structure and compiler design. He is currently working as Assistant professor in department of CSE in S.A Engg college, Chennai.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013