INNOVATIVE SCIENCE AND TECHNOLOGY PUBLICATIONS

International Journal of Future Innovative Science and Technology
ISSN: 2454- 194X Volume - 2, Issue - 2

Manuscript Title

# A PACKET DROPPING ATTACK DETECTION FOR WIRELESS AD HOC NETWORK USING KEY MANAGEMENT

[1] P.S.Kirthana, [2] Yasotha B.E.,M.Tech.,

P.G Scholar, Assistant Professor,

Department of Computer Science and Engineering,

MNM Jain Engineering College Chennai

E-Mail: kirthy.selva@gmail.com, yasotha.mnm@gmail.com

**May – 2016**

www.istpublications.com

International Journal of Future Innovative Science and Technology, ISSN: 2454- 194X
Volume-2, Issue-2, May - 2016 editor@istpublications.com

# A PACKET DROPPING ATTACK DETECTION FOR WIRELESS AD HOC NETWORK USING KEY MANAGEMENT

[1] P.S.Kirthana, [2] Yasotha B.E.,M.Tech.,

P.G Scholar, Assistant Professor,
Department of Computer Science and Engineering,
MNM Jain Engineering College Chennai
E-Mail: kirthy.selva@gmail.com, yasotha.mnm@gmail.com

## ABSTRACT

**A fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Unfortunately, this kind of technique consumes much energy and hence largely limits the lifespan of WSN. The Secure and Efficient data Transmission protocol for WSNs, called IBS, by using the Identity-Based digital Signature (IBS) scheme. In IBS, the security relies on the hardness of the Diffie-Hellman problem in the pairing domain. The feasibility of the IBS protocol with respect to the security requirements and security analysis against various attacks. In exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To calculate the correlation between these lost packets, it is critical to acquire truthful packet-loss information at individual nodes. The calculations and simulations are provided to illustrate the efficiency.**

***Index terms –*** *Packet dropping attack, Identity-Based digital signature, insider attack, malicious nodes, wireless sensor network.*

## I. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying routing traffic. An adversary can exploit this cooperative nature to launch attacks. Once being included in a route, the adversary starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination. Eventually, such a severe denial-of-service (DoS) attack can paralyze the network by partitioning its topology.Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages. First, the continuous presence of extremely high packet loss rate at the malicious nodes makes this type of attack easy to be detected. Second, once being detected, these attacks are easy to mitigate. If the malicious nodes are also identified, their threats can be completely eliminated by simply deleting these nodes from the network's routing table.

A malicious node that is part of the route can exploit its knowledge of the network protocol and the communication context to launch an insider attack—an attack that is intermittent, but can achieve the same performance degradation effect as a persistent attack at a much lower risk of being detected. Specifically, the malicious node may evaluate the importance of various packets, and then drop the small amount that are deemed highly critical to the operation of the network. In particular, we are interested in the problem of detecting the occurrence of selective packet drops and identifying the malicious nodes responsible for these drops. Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional. Specifically, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions or by the insider attacker.

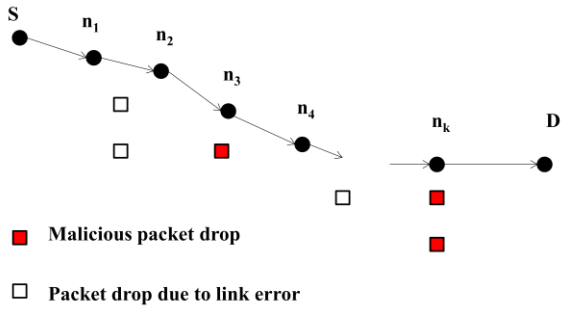


Figure 1. Network and attack model.

Every node maintains a routing table which stores the next hop, cost metric towards each destination. A sequence

number that is created by the destination itself. Each node periodically forwards routing table to its neighbors to select route to reach destination. Smart grid is an emerging cyber-physical system that incorporates networked control mechanisms into conventional power infrastructures. To defend against jamming attacks is of critical importance to secure wireless communications in the smart grid. Interesting enough, most efforts adopt a case-by-case methodology to investigate how a message can be sent to its destination. In other words, based on commonly-adopted jamming attack models existing works focus on designing anti-jamming communication schemes for message delivery in conventional wireless networks.

Consider two general jamming-resilient communication modes for smart grid applications: coordinated and uncoordinated modes. In coordinated mode, the sender and receiver share a common secret or key (e.g., code-frequency channel assignment), which is unknown to attackers. Accordingly, an attacker has to choose its own strategy to disrupt the communication between the transmitter and receiver. Coordinated communication is a conventional model in spread spectrum systems. The transmitter and receiver may not share a common secret initially (e.g., a node joins a network and attempts to establish a secret with others). Uncoordinated communication is therefore used to help establish such an initial key. The mathematical derivations, that the worst-case performance in terms of message invalidation probability exhibits a U-shaped response to aggregated network traffic load.

Based on this U-shape effect, a transmitting adaptive camouflage traffic (TACT) system that uses “camouflage traffic” to achieve the optimal aggregated network traffic load to minimize the message invalidation ratio. The underlying explanation behind the U-shape phenomenon and the TACT anti-jamming strategy is that using camouflage traffic to the network, we can force a jammer to “waste” enough jamming capability on the camouflage traffic (because the jammer has no way to tell the camouflage traffic from the real smart grid traffic), so that the jammer cannot find the real traffic quickly enough. The strategy is based on the worst-case methodology, the U-shape property and the global minimum of the message invalidation probability are independent with a particular jamming strategy, thus offering performance guarantee for a wireless smart grid application under jamming attacks.

## II RELATED METHODS

[1] Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores ale. Previous work has shown that proofs of storage can be constructed from any homomorphic linear authenticator (HLA). The latter, roughly speaking, are signature/message authentication schemes where `tags' on multiple messages can be homomorphically combined to yield a `tag' on any linear combination of these messages. A framework for building public-key HLAs from any identification protocol satisfying certain homomorphic properties. Then show how to turn any public-key HLA into publicly-variable PoS with communication complexity independent of the file length and supporting an unbounded number of verifications. The use of our transformations by applying them to a variant of an identification protocol by Showup, thus obtaining the first unbounded-use PoS based on factoring (in the random oracle model).

[2] Adhoc networks offer increased coverage by using multi-hop communication. The 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. The impact of several Byzantine attacks performed by individual or colluding attackers. The ODSBR, first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link after log n faults have occurred, where n is the length of the path. Problematic links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. The protocol never partitions the network and bounds the amount of damage caused by attackers. It demonstrate through simulations ODSBR’s effectiveness in mitigating Byzantine attacks. The 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 multi-hop wireless routing protocols.

[3] A short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves. The signature length is half the size of a DSA signature for a similar level of security. The short signature scheme is designed for systems where signatures are typed in by a human or signatures are sent over a low-bandwidth channel.

[4] In military and rescue applications of mobile ad hoc networks, all the nodes belong to the same authority; therefore, they are motivated to cooperate in order to support the basic functions of the network. In this paper, we consider the case when each node is its own authority and tries to maximize the benefits it gets from the network. More precisely, assume that the nodes are not willing to forward packets for the benefit of other nodes. These

problem may arise in civilian applications of mobile ad hoc networks. In order to stimulate the nodes for packet forwarding, we propose a simple mechanism based on a counter in each node. The behavior of the proposed mechanism analytically and by means of simulations, and detail the way in which it could be protected against misuse.

[5] Security is a critical problem when implementing Mobile Ad Hoc Networks (MANETs) and is widely acknowledged. It describes the effects of selfish nodes in MANETs. An Ad Hoc Network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services. One of the different kinds of misbehavior is node selfishness. A selfish node wants to preserve its own resources while using the services of others and consuming their resources, such misbehaving nodes participate in the route discovery and maintenance phase but refuse to forward data packets, which degrades routing performance. An authenticated scheme, which preserves communication privacy and mitigates selfish nodes in MANETs.

**III PROPOSED SYSTEM**

The proposed system is to efficiently find the packet dropping attack that happen between the nodes and minimize these attack using key management

The System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose Secure and Efficient data Transmission protocol for WSNs, by using the Identity-Based digital Signature (IBS) scheme, respectively. It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the digital signature initially.

1. These techniques will provide the effective methods of detecting the packet dropping attack happened between the nodes.

2. The TACT will help to reduce the packet loss between the nodes.

3. Applying Digital signatures to message packets are efficient in communication and applying the key management for security.

The subsequent section are organized as follows Architecture, Smart Grid Network, Jamming Attack, Worst case methodology, Block based Detection, Tact.

**ARCHITECTURE**

In this paper we propose an architecture that detects the packet dropping attack in a smart grid network by jammer during packet forwarding at the network load, the nodes share the secret key to detect the packet drop by the block based method, and Tact methodology will be used to overcome these packet dropping attack.

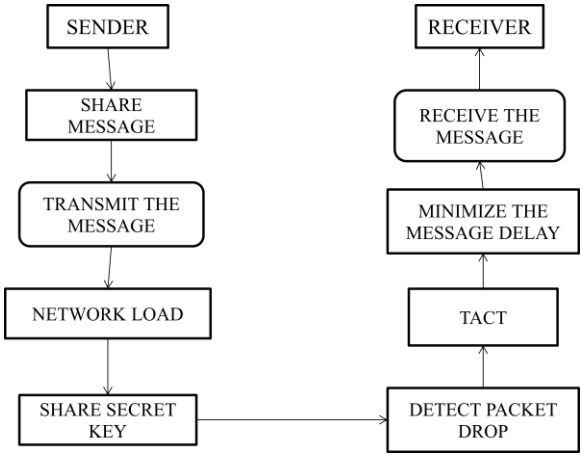


Figure - 2. System Architecture.

A. SMART GRID NETWORK

Each node maintains a routing table which stores. Next hop, cost metric towards each destination. A sequence number that is created by the destination itself. Each node periodically forwards routing table to its neighbors to select route to reach destination. When the route request is reached to Destination, it selects the route as best to communication and maintains the route for source to destination communication.

B. JAMMING ATTACK

Smart grid is an emerging cyber-physical system that incorporates networked control mechanisms (e.g., advanced metering and demand response) into conventional power infrastructures. To facilitate information delivery for such mechanisms, wireless networks that provide flexible and untethered network access have been proposed and designed for a variety of smart grid applications primary security threat to prevent the deployment of wireless networks for the smart grid. There have been extensive works on designing spread spectrum based communication schemes, which provide jamming resilience to conventional wireless networks by using multiple orthogonal frequency

or channels. A case-by-case (or model-by-model) methodology to investigate how a message can be sent to its destination. Based on commonly-adopted jamming attack models (e.g., periodic, memory less, and reactive models), existing works focus on designing anti-jamming communication schemes for message delivery in conventional wireless networks.

C. WORST CASE METHODOLOGY

The widely-used case-by-case methodology cannot be readily adapted to wireless smart grid applications, because it is not able to guarantee reliable communication under any potential jamming attack. To provide such a guarantee, securing wireless smart grid applications requires a paradigm shift from the case-by-case methodology to a new worst-case methodology that offers performance assurance under any attack scenario. Address this issue by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for smart grid applications. Two general jamming-resilient communication modes for smart grid applications, coordinated and uncoordinated modes. In coordinated mode, the sender and receiver share a common secret or key (e.g., code-frequency channel assignment), which is unknown to attackers. Accordingly, an attacker has to choose its own strategy to disrupt the communication between the transmitter and receiver. Coordinated communication is a conventional model in spread spectrum systems. Uncoordinated communication is therefore used to help establish such an initial key. In uncoordinated communication, the sender and receiver randomly choose a frequency-code channel to transmit and receive, respectively. A message can be delivered from the sender to the receiver only if they both reside at the same channel, and at the same time the jammer does not disrupt the transmission on the channel. The worst-case performance under a generic (rather than specific) jamming process. Through mathematical derivations, that the worst-case performance in terms of message we propose to study the worst-case performance under a generic (rather than specific) jamming process.

D. BLOCK BASED DETECTION

Most of the computation is done at the source node (for generating HLA signatures) and at the public auditor (for conducting the detection process). The public auditor as a dedicated service provider that is not constrained by its computing capacity. So the computational overhead should not be a factor limiting the application of the algorithm at the public auditor. On the other hand, the proposed algorithm requires the source node to generate K HLA signatures for a K-hop path for each data packet. The generation of HLA signatures is computationally expensive, and may limit the applicability of the algorithm. One solution to this problem is to make the signature scalable, e.g., instead of generating a per-packet signature, a per-block signature may be generated, where each block has L packets. Accordingly, the detection will be extended to blocks (a block is defined as lost if a packet in the block is lost).

E. TACT

A transmitting adaptive camouflage traffic (TACT) system that uses “camouflage traffic” to achieve the optimal aggregated network traffic load to minimize the message invalidation ratio. The underlying explanation behind the U-shape phenomenon and the TACT anti-jamming strategy is that using camouflage traffic (i.e., redundant traffic transmitted by TACT) is the over-provision of bandwidth in a smart grid network, where time critical traffic rate is smaller than the network bandwidth. By sending more such camouflage traffic (mixed with smart grid control traffic) to the network, we can force a jammer to “waste” enough jamming capability on the camouflage traffic (because the jammer has no way to tell the camouflage traffic from the real smart grid traffic), so that the jammer cannot find the real traffic quickly enough. Therefore, the message invalidation ratio decreases when we send camouflage traffic into the network under jamming. However, if the rate of sending camouflage traffic keeps increasing and approaches the network bandwidth, more network collisions will happen in the network, thereby degrading the network performance (i.e., increasing the message invalidation ratio). As a result, there exists an optimal rate to send camouflage traffic and TACT is used to adaptively find this rate. Because our strategy is based on the worst-case methodology, the U-shape property and the global minimum of the message invalidation probability are independent with a particular jamming strategy, thus offering performance guarantee for a wireless smart grid application under jamming attacks.

## IV CONCLUSION

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required. Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. A decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as router in wired networks

or access point in managed (infrastructure) wireless networks. Instead, participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multihop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders.

**V REFERENCES**

[1] Ateniese G., Kamara S. and Katz J. (2009), 'Proofs of storage from homomorphic identification protocols'.

[2] Awerbuch B., Curtmola R., Holmer D., Nita-Rotaru C. and Rubens H. (2008), 'ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks'.

[3] Balakrishnan K., Deng J. and Varshney P.K. (2005), 'TWOACK: Preventing selfishness in mobile ad hoc networks'.

[4] Boneh D., Lynn B. and Shacham H. (2004), 'Short signatures from the weil pairing'.

[5] Buchegger S. and Boudec J.Y.L. (2002), 'Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)'.

[6] Buttyan L. and Hubaux J.P. (2003), 'Stimulating cooperation in selforganizing mobile ad hoc networks', ACM/Kluwer Mobile Netw.

[7] Galuba W., Papadimitratos P., Poturalski M., Aberer K., Despotovic Z., and Kellerer W. (2010), 'Castor: Scalable secure routing for ad hoc networks'.

[8] Gunasekaran M., Sampath P., Gopalakrishnan B. (2009) 'Aas: An Authenticated Acknowledgement-Based Scheme For Preventing Selfish Nodes In Mobile Ad Hoc Networks'.