**Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks**

**ABSTRACT:**

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, we verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

**EXISTING SYSTEM:**

* The most of the related works preclude the ambiguity of the environment by assuming that malicious dropping is the only source of packet loss, so that there is no need to account for the impact of link errors. On the other hand, for the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve an acceptable detection accuracy.
* Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories.
* The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping.
* The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

**DISADVANTAGES OF EXISTING SYSTEM:**

* In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. This problem has not been well addressed in the existing system.
* In the existing system first category case, the impact of link errors is ignored.
* In the second Category, Certain knowledge of the wireless channel is necessary in this case.

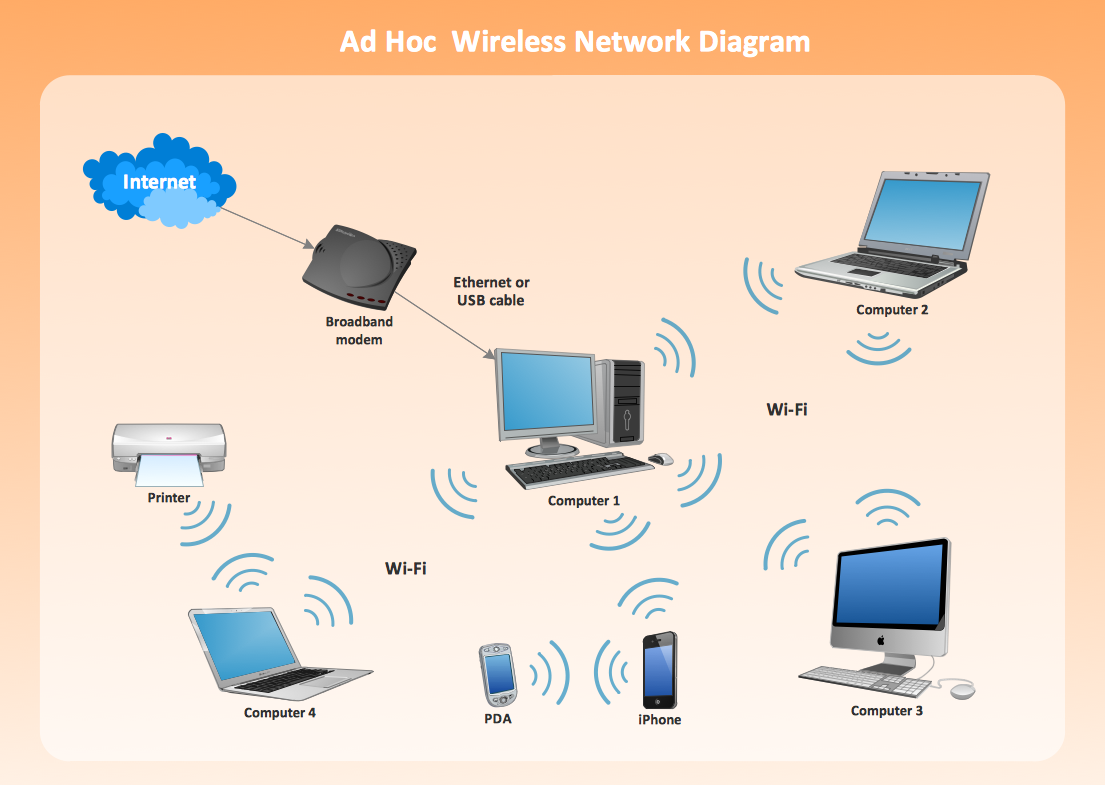
**PROPOSED SYSTEM:**

* In this paper, we develop an accurate algorithm for detecting selective packet drops made by insider attackers.
* Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.
* The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.
* Our algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The proposed system with new HLA construction is collusion-proof.
* The proposed system gives the advantage of privacy-preserving.
* Our construction incurs low communication and storage overheads at intermediate nodes. This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue.
* Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

**SYSTEM ARCHITECTURE:**



**BLOCK DIAGRAM:**

****

**BLOCK DIAGRAM:**



**Wireless Ad hoc Network**

**Source**

**Destination**

**Packet Drop**

**Packet Transmission**

**Link Failure**



**Wireless Ad hoc Network**

**Source**

**Destination**

**HLA Scheme – Link Failure Detection**

**Packet Transmission**

**MODULES:**

* Network Configuration
* Homomorphic Linear Authenticator
* Setup Phase and Packet Transmission Phase
* Audit Phase and Detection Phase

**MODULES DESCRIPTION:**

**Network Configuration**

In this project we are using Wireless Adhoc Network. Here we mainly focus on static or quasi-static network. In wireless network we need to send the packet through the node. System is represented as a node. Here every node has communication range. By using this range only we can transmit over packet. If source and destination node exists within the communication range, source can directly transmit the packet. Otherwise, we need to select the intermediate node based on the transmission range for transmit the packets.

**Homomorphic Linear Authenticator**

To correctly calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. We use HLA cryptographic primitive for this purpose. The basic idea of our method is as follows. An HLA scheme allows the source, which has knowledge of the HLA secret key, to generate HLA signatures s1, . . , sMfor M independent messages r1, . . . , rM, respectively. The HLA signatures are made in such a way that they can be used as the basis to construct a valid HLA signature for any arbitrary linear combination of the messages, , without the use of the HLA secret key, where *ci*’s are randomly chosen coefficients. A valid HLA signature for , can be constructed by a node that does not have knowledge of the secret HLA key if and only if the node has full knowledge of *s*1*, . . . , sM*. So, if a node with no knowledge of the HLA secret key provides a valid signature for ,, it implies that this node must have received all the signatures *s*1*, . . . , sM*.

**Setup Phase and Packet Transmission Phase**

This phase takes place right after route PSD is established, but before any data packets are transmitted over the route. In this phase, S decides on a symmetric-key crypto-system (encrypt key, decrypt key) and K symmetric keys key1, . . . , keyK, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S securely distributes decrypt key and a symmetric key keyj to node nj on PSD, for j = 1, . . . ,K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts keyj using the public key of node nj and sends the cipher text to nj . nj decrypts the cipher text using its private key to obtain keyj .

After completing the setup phase, *S* enters the packet transmission phase. Before sending out a packet *Pi*, where *i* is a sequence number that uniquely identifies *Pi*, *S* computes *ri* = *H*1(*Pi*) and generates the HLA signatures of *ri* for node *nj* , as follows

sji = [H2(i||j)uri ]x, for j = 1, . . . ,K

where || denotes concatenation. These signatures are then sent together with Pi to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes.

**Audit Phase and Detecting Phase**

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1, . . . , nK, S’s HLA public key information pk = (v, g, u), the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest.

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : JAVA
* IDE : Netbeans 7.4

**REFERENCE:**

Tao Shu and Marwan Krunz, “Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, **IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, APRIL 2015.**