**DETECTION OF PACKET DROPPING ATTACKS IN**

**WIRELESS ADHOC NETWORK**

B.KOWSALYA, K.NITHIN, G.T.PRASATH

##### ABSTRACT

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. While observing a sequence of packet losses in the network, whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop is to be identified. 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, the correlations between lost packets is identified. Homomorphic linear authenticator (HLA) based public auditing architecture is developed 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.

**INTRODUCTION**

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. In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories. The first sub-category is based on credit systems. A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a malicious node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

**PROJECT DESCRIPTION**

**EXISTING SYSTEM**

The first category aims at high malicious dropping rates, where most, or all of the lost packets are caused only by malicious dropping. In this case, the impact of link errors is ignored. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories.

* **Credit System**

A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

* **Reputation System**

A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route.

* **End-To End or Hop-To-Hop Acknowledgement**

To directly locate the hop where packets are lost. A hop of high packet loss rate will be excluded from the route.

* **Cryptographic Methods**

Bloom filters used to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates.

**DISADVANTAGE**

* Exceed resource constraints.
* High trust evaluation cost.
* Depend on specific routing scheme, platform
* Doesn’t suite for large scale network.

**PROPOSED SYSTEM**

The proposed Privacy-Preserving and Truthful Detection are with two topologies. One is the intra-group topology where distributed trust management is used. The other is inter-group topology where centralized trust management approach is employed. For the intra-group network, each sensor that is a member of the group, calculates individual trust values for all group members.

Based on the trust values, a node assigns one of the three possible states:

1) trusted,

2) un-trusted or

3) un-certain to other member nodes.

This three-state solution is chosen for mathematical simplicity and is found to provide appropriate granularity to cover the situation. After that, each node forwards the trust state of all the group member nodes to the CH. Then, centralized trust management takes over. Based on the trust states of all group members, a CH detects the malicious node(s) and forwards a report to the base station. On request, each CH also sends trust values of other CHs to the base station. Once this information reaches the base station, it assigns one of the three possible states to the whole group. On request, the base station will forward the current state of a specific group to the CHs.

Our group based Privacy-Preserving and Truthful Detection in three phases:

1) Trust calculation at the node level,

2) Trust calculation at the cluster head level, and

3) Trust calculation at the base station level.

**A. TRUST CALCULATION AT THE NODE LEVEL**

At the node level, a trust value is calculated using either time-based past interaction or peer recommendations. Whenever a node y wants to communicate with node x, it first checks whether y has any past experience of communication with x during a specific time interval or not. If yes, then node x makes a decision based on past interaction experience, and if not, then node x moves for the peer recommendation method.

***1) Time-based Past Interactions Evaluation***

Trust calculation at each node measures the confidence in node reliability. Here the network traffic conditions such as congestion, delay etc., should not affect the trust attached to a node; this means that the trust calculation should not emphasize the timing information of each interaction too rigidly. Therefore, we introduce a sliding time window concept which takes relative time into consideration and reduces the effects of network conditions on overall trust calculation. If real-time communication is a requirement, as is the case in most real world applications, this timing window concept does not provide any hindrance when it comes to real-time delivery of packets. The communication protocol in such applications is always accompanied with time-stamps, and thus any node which delays the delivery of packets by taking advantage of the sliding timing window will be detected straightforwardly.

**2) *Peer Recommendations Evaluation***

Let a group be composed of n uniquely identified nodes. Furthermore, each node maintains a trust value for all other nodes. Whenever a node requires peer recommendation it will send a request to all member nodes except for the un-trusted ones. Let us assume that j nodes are trusted or uncertain in a group.

**B. TRUST CALCULATION AT THE CLUSTER-HEAD LEVEL**

Here we assume that the CH is the SN that has higher computational power and memory as compared to other SNs.

**1) *Trust State Calculation of Own Group***

In order to calculate the global trust value of nodes in a group, CH asks the nodes for their trust states of other members in the group. We use the trust states instead of the exact trust values due to two reasons. First, the communication overhead would be less as only a simple state is to be forwarded to the CH. Secondly, the trust boundaries of an individual node vary from other nodes. A particular trust value might be in a trusted zone for one node whereas it may only correspond to the uncertain zone for another node. Hence the calculation of the global trust state of nodes in a group would be more feasible and efficient if we only calculate it using the trust states.

***2) Trust Calculation of Other Groups***

During group-to-group communication, the CH maintains the record of past interactions of another group in the same manner as individual nodes keep record of other nodes. Trust values of a group is calculated on the basis of either past interaction or information passed on by the base station. Here we are not considering peer recommendations from other groups in order to save communication cost.

***C. Trust Calculation at Base Station Level***

The base station (BS) also maintains the record of past interactions with CHs in the same manner as individual nodes. On reception of trust vectors from all the CHs, the base station will calculate the trust value of each group in a manner

**ADVANTAGES**

* Task sharing.
* Cluster Head (CH) identifies the false nodes.
* In multi hop case it selects trusted en-route.
* In inter-cluster communication it selects trusted gateway.
* The proposed system with HLA construction provides collusion-proof.

**ACTIVITY DIAGRAM**

Login

Client Request

Request file

Cluster connected

Path generated

Packet send

Received packet

Merged packet

Received files

If Valid

Error

message

if Invalid

**DESCRIPTION**

Activity diagrams are graphical representations of work flows of step wise activities and actions with support for choice, iteration and concurrency. In the unified modeling language, activity diagrams can be used to describe the business and operational step by step work flows of components in a system. An activity diagram shows the overall flow of control

**SYSTEM SPECIFICATION**

**HARDWARE SPECIFICATION**

Processor : Any Processor above 500 MHz

Ram : 128Mb.

Hard Disk : 10 GB.

Compact Disk : 650 Mb.

Input device : Standard Keyboard and Mouse.

Output device : VGA and High Resolution Monitor.

**SOFTWARE SPECIFICATION**

Operating System : Win2000/XP / Linux 9.0

Programming Package : C# .Net

Tools : Visual Studio.

**CONCLUSION AND FUTURE WORKS**

**CONCLUSION**

Recommendation scenario during simulation, in each cluster with the emergence of widespread use of WSNs, the need random number of source nodes are selected which perform of a proper trust management scheme is strongly felt in this peer recommendation with the other nodes. Also, each cluster work, we have proposed a robust lightweight group-based trust head will perform peer recommendation with neighboring management scheme Privacy-Preserving and Truthful Detection for clustered WSNs.

**FUTURE WORK**

As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy preserving requirement for the auditing process, and the randomness of wireless channels and packet losses, but ignore the particular behaviour of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in future studies.

**REFERENCE**

1. D. B. Johnson, D. A. Maltz, and J. Broch, 2001, DSR: the dynamic source routing protocol for multi-hop wireless ad-hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172.
2. G. Noubir and G. Lin, July 2003, Low-power DoS attacks in data wireles lans and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30.
3. L. Buttyan and J. P. Hubaux, Oct.2003 Stimulating cooperation inself-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5):579–592.
4. W. Xu, W. Trappe, Y. Zhang, and T. Wood, 2005, The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57.
5. J. Eriksson, M. Faloutsos, and S. Krishnamurthy, 2007, “Routing amid colluding attackers,” in Proc. IEEE Int. Conf. Netw. Protocols, pp.
6. W.Kozma and L.Lazos,2009,REACT: Resource-Efficient Accountability for node misbehavior in ad hoc networks based on random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec).
7. A. Proano and L. Lazos, 2010, Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6.