International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com Volume – 1. Issue – 1. November 2014

TOWARD PRIVACY PRESERVING AND COLLUSION RESISTANCE IN A LOCATION PROOF UPDATING SYSTEM

R.Bhuvaneswari[1], V.Vijayalakshmi [2]

[1]M.Phil., Scholar, Bharathiyar Arts And Science College For Women, India

[2] HOD Cum Assistant Professor, Bharathiyar Arts and Science College for Women, India

[1]bhuvanapriyamca@gmail.com, [2]vijisylvia@gmail.com,

Abstract : **In computing area the Location-Based services take advantage of user location information and provide mobile users with various resources and services. The common theme across these location sensitive applications is that they offer a reward or benefit to users located in a certain geographical location at a certain time. Thus, users have the incentive to cheat on their locations. Location-sensitive applications require users to prove that they really are (or were) at the claimed locations. Nowadays, more and more location-based applications and services require users to provide location proofs at a particular time. Mobile users have devices capable of discovering their locations, some users may cheat on their locations and there is a lack of secure mechanism to provide their current or past locations to applications and services. One possible solution is to build a trusted computing module on each mobile device to make sure trusted GPS data is generated and transmitted. Although cellular service providers have tracking services that can help to verify the locations of mobile users in real time, the accuracy is not good enough and the location history can not be verified.**

INTRODUCTION

Recently, several systems have been designed to let end users prove their locations through WiFi infrastructures. We propose A Privacy-Preserving Location proof Updating System (APPLAUS), which does not rely on the wide deployment of network infrastructure or the expensive trusted computing module. In APPLAUS, Bluetooth enabled mobile devices in range mutually generate location proofs, which are used for trusted location to monitor the proof server. Mobile nodes communicate with neighboring nodes through Bluetooth and communicate with the untrusted server through the cellular network interface. According to Location proof updating system based on different roles they play in the process of location proof updating, they are categorized as Prover, Witness, Location Proof Server, Certificate Authority or Verifier. For control forwarding packet loss from the Disruption tolerant networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Due to a lack of consistent connectivity, two nodes exchange data only when they move into the transmission range of each other (which is called a contact between them). Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets and also power loss and buffer overflows. To demonstrate this, we simulate the effects of routing misbehavior in two popular DTN routing algorithms, SimBet and Delegation based on the Reality trace.

Then we propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes. Introduces both routing and security model for examine those nodes from packet loss. By this mechanism we control the packet loss and also used more specifically, we use statistically updated pseudonyms at each mobile device to protect location privacy from each other, and from the untrusted location proof server.

For CA verification, we use TKIP (temporal key integrity protocol), it's a security protocol used in mobile adhoc networks(IEEE 802.11).It has wireless network standards and designed to focus on encryption of data/packets in location proof systems. In order to defend against colluding attacks, we also present betweenness ranking-based and correlation clustering-based approaches for outlier detection. An extensive experimental and simulation result based on multiple data sets show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks and also avoids packet loss by mitigation detection scheme. Atlas, implementation shown in simulation results.

PROBLEM IDENTIFACTION AND SOLUTION

In wireless network location proof updating system faces packet loss problems and We develop a mobile station with user-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof request.To transfer the data packet from source to destination commonly user TCP/IP protocol in networking. In this TCP/IP process is before transfer the data the connection has been established.

Each node forwards the query to the next node. During the lookup process no information is send back to the originator, resulting in less packet overhead. To make the routing strategy perform best, we present an efficient routing strategy, called tracer routing. Tracer routing enables the initiator to trace the whole routing process. To detect the packet loss and reduce the traffic occurs in network we use DTN and Mitigating scheme technique and use encryption mechanism to update the pseudonyms statistically.

PROBLEM DESCRIPTION

MODULES

- Mobility Network Formation Module
- User Interface Design
- Routing and Security Model
- Record Summary and Contact Record
- Witeness Node - Misreporting Detection
- Black List

MOBILITY NETWORK FORMATION MODULE

We contribute to a more systematic understanding and treatment of sensor deployment issues. For this purpose, we studied the existing literature on deployment experience and present a classification of common problems encountered during deployment of sensor networks. A wireless network that is temporarily installed alongside the actual sensor network during the deployment process. Parameters considered during sensor network formation

- **Transmission range:** nodes communication depends under transmission range which is placed nearly close to each other thus gets better link.
- **Local information system:** Nodes must be grouped under specific feature like battery power, processing capability, bandwidth, memory etc. so according to those, nodes are partitioned using driver methods.
- **Mobility:** Mobility refers the node movement procedure so need to consider the mobility options with limitation in maximum and minimum speed.

USER INTERFACE DESIGN

- The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements (e.g., mental model) to create a system that is not only operational but also usable and adaptable to changing user needs.

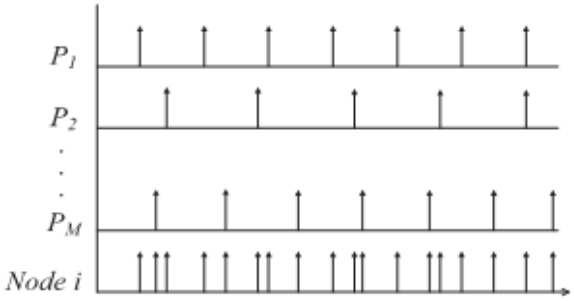

Fig 1 Updation of User Nodes

ROUTING AND SECURITY MODEL

We describe each node has two separate buffers. One has unlimited space and is used to store its own packets; the other one has limited space and is used to store packets received from other nodes. We determine the network is loosely synchronized; i.e., any two nodes should be in the same time slot at any time. Since the intercontact time is usually at the scale of minutes or hours, the time slot can be at the scale of one minute. Thus, such loose time synchronization is not hard to achieve.There are two types of nodes: misbehaving nodes and normal nodes. A misbehaving node drops the received packets even if it has available buffers,1 but it does not drop its own packets. It may also drop the control messages of our detection scheme. We assume a small number of misbehaving nodes may collude to avoid being detected, and they may synchronize their actions via out-band communication channels.In some Mobile stations, each packet has a certain lifetime, and then expired packets should be dropped whether or not there is buffer space. Such dropping can be identified if the expiration time of the packet is signed by the source. We assume a public-key authentication service is available. In identity-based authentication, only the offline trusted private key generator can generate a public/private key pair, so a misbehaving node itself cannot forge node identified and detected by using APPLAUS and DTD Mechanism and also helpful to give indications to other nodes.

RECORD SUMMARY AND CONTACT RECORDS

The two nodes also exchange their current vector of buffered packets (as a step of contact record generation). In this way, one node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted by and , respectively. It also knows the two sets of packets the other node sends and receives in the previous contact, which are denoted by and a misbehaving node may drop a packet but keep the packet ID, pretending that it still buffers the packet. The next contacted node may be a better relay for the dropped packet according to the routing protocol, which can be determined when the two exchange the destination (included in packet ID) of the buffered packets. In this case, the misbehaving node should forward the packet to the next contacted node, but it cannot since it has dropped the packet in such cases we use an in order to defend against colluding attacks, and betweenness ranking-based and correlation clustering-based approaches for outlier detection. Thus, the next contacted node can easily detect this misbehavior and will not forward packets to this misbehaving node.

WITENESS NODE - MISREPORTING DETECTION

Detection: To detect the inconsistency caused by misreporting, for each contact record generated and received in a contact, a node selects random nodes as the witness nodes of this record, and transmits the summary of this record to them when it contacts them. It selects the witness nodes from the nodes that it has directly contacted. Here, the nodes contacted a long time ago are not used since they may have left the network.

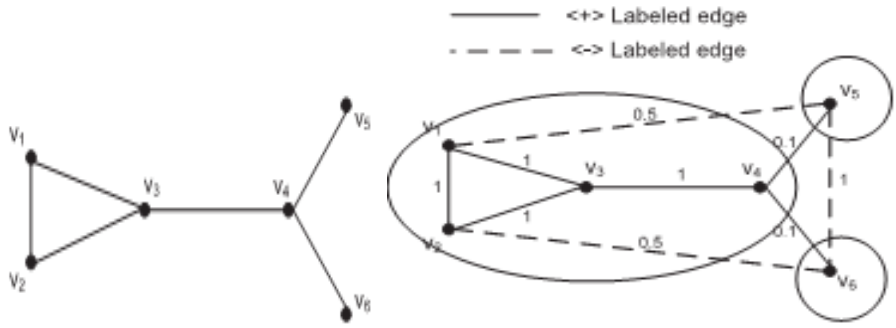

Fig 2 Detection of Nodes in Network Shown In Graphs.

- **Alarm:** After detection, the witness node floods an alarm to all other nodes. The alarm includes the two inconsistent summaries. When a node receives this alarm, it verifies the inconsistency between the included summaries and the signature of the summaries. If the verification succeeds, this node adds the appropriate misreporting node into a blacklist and will not send any packets to it. If the verification fails, the alarm is discarded and will not be further propagated. A misreporting node will be kept in the blacklist for a certain time before being deleted.
- A node deletes the record that it generates in a contact after the contact has been purged out of its report window, probably after a few contacts. It deletes the records received from the contacted node right after this contact, since these received records are only used to check if the contacted node has dropped packets recently. The witness node should keep its collected record summaries for a long enough time to detect misreporting. For simplicity, our scheme uses a time-to-live parameter, which denotes the time for the collected summaries to be stored before being deleted.

BLACK LIST

To mitigate routing misbehavior, we try to reduce the number of packets sent to the misbehaving nodes. If a node is detected to be misreporting, it should be blacklisted and should not receive packets from others. We cannot simply blacklist it because it is dropping packets, since a normal node may also drop packets due to buffer overflow. So we used mitigating routing and detection scheme used in this case and we focus on how to detect nodes from without affecting and normal nodes from misreporting.

Our basic idea is to maintain a metric forwarding probability (FP) for each node based on if the node has dropped, received and forwarded packets in recent contacts, which can be derived from its reported contact records. The nodes that frequently drop packets but seldom forward packets will have a small FP and will receive few packets from others. Our scheme borrows ideas from congestion control to update FP. More specifically, it combines additive increase, additive decrease, and multiplicative decrease to differentiate misbehaving nodes from normal nodes.

CONCLUSION

A privacy-preserving location proof updating system called APPLAUS, where collocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location from the untrusted location proof server. We presented a scheme to detect packet dropping in DTNs. The detection scheme works in a distributed way, each node detects packet dropping locally based on the collected information. Analytical results on detection probability and detection delay were also presented. We also develop a user-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To deal with colluding attacks, we proposed betweenness ranking based and correlation clustering-based approaches for outlier detection. Moreover, the detection scheme can effectively detect misreporting even when some nodes collude. Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively.

The proposed scheme is very generic and it does not rely on any specific routing algorithm. Trace-driven simulations show that our solutions are efficient. Moreover, it preserves source location privacy and it is collusion resistant.

REFERENCES

[1] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, 2003.

[2] U. Brandes, "A Faster Algorithm for Betweenness Centrality," J. Math. Sociology, vol. 25, no. 2, pp. 163-177, 2001.

[3] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93), 1994.

[4] L. Buttya ´n, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks, 2007.

[5] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.

[6] L.P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: Flexible Privacy Controls for Presence-Sharing," Proc. ACM MobiSys, 2007.