MISBEHAVIOR REPORT AUTHENTICATION SCHEME FOREFFICIENT AUTHENTICATION IN WIRELESS MOBILE NETWORK.

[1]Priya.T, [2]S.Ramesh.
[1]Research Scholar, Department of Computer Science, Paavai College of Engineering, Namakkal,Tamilnadu, India.
[2]Assistant Professor, Department of Computer Science, Paavai College of Engineering, Namakkal,Tamilnadu, India.

Abstract: Secure authentication in wandering services is being designed to allow legal users to get access to wireless network services when they are away from their home location. In recent times, to keep the location privacy of users, there have been researches on nameless validation. In particular, nameless verification without the involvement of home servers has attracted significant interest owing to its influence on the communication efficiency. The MRA (Misbehavior Report Authentication) scheme is designed to resolve the weakness of existing when it fails to detect misbehaving nodes with the occurrence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report genuine nodes as malicious. This attack can be dangerous to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The source route broadcasts an RREQ message to all the neighbors within its transmission range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

1. INTRODUCTION

A geographic transmission schemes use an ad hoc design for the protocol that selects the relay node. These existing protocols typically employ one of the following two strategies. One strategy is to equip users with a large number of authenticated pseudonyms. Then, users use authenticated pseudonyms to communicate in these ad-hoc networks so that their real identities are hidden from peer users. In most of such approaches, there are two major limitations. First, the server which produces the pseudonyms can track the users. Second, the revocation of the long list of pseudonyms of a malicious user is very costly.

Existing geographic transmission schemes use an ad hoc design for the protocol that selects the relay node. These existing protocols typically employ one of the following two strategies. One strategy is to equip users with a large number of authenticated pseudonyms. Users use authenticated pseudonyms to communicate in these ad-hoc networks so that their real identities are hidden from peer users. Weak anonymity and insecurity in the CK model.disadvantageThe server which produces the pseudonyms can track the users. Backward link ability and leakage of the session key or inefficient operations. The revocation of the long list of pseudonyms of a malicious user is very costly. Proposed system The MRA (Misbehavior Report Authentication) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the

source node by reversing the route in the RREQ message. It helps to communicate securely. Both the sender and receiver get authentication through this method. Advantages The results show that the proposed scheme is robust to packet loss and can succeed when various network jitter patterns exist.

Little impact is found on the performance of the application. Over the Internet, the experiments are performed on nodes with 16-hop distance.

2.Related work

Verifier-Local Revocation Group Signature Schemes with Backward Un link ability from Bilinear Maps Consider a k-ary tree with two levels for an integer k s.t. T · k2 (see Fig. 1). Although author show only the case of two levels, the extension to more levels is easy. In the tree, the root node is N0, Nj1 is the j1-th child of N0, and Nj1j2 is the j2-th child of Nj1 , for j1; j2 2 [1; k]. Each node Nj1 is assigned to hj1 2R G, and each node Nj1j2 is assigned to hj1j2 2R G. In this situation, every interval j 2 [1; T] can be correspondent to a pair of two indexes j1 and j2 for j1; j2 2 [1; k] such that j = j1k + j2. Then, the next interval of (j1; j2) is (j1; j2 + 1) unless j2 6= k, and if j2 = k, the next interval is (j1 +1; 1). In each interval (j1; j2), the values hj1 and hj1j2 along the path are used. VLR group signature scheme based on bilinear maps is proposed by Boneh and Shacham. The advantage of this scheme is that signatures are short, since the elliptic curves can be adopted. On the other hand, the schemes have an advantage over backward unlinkability. This property means that even after a member is revoked, signatures produced by the member before the revocation remain anonymous. However, in the scheme of all the signatures produced from the revoked member are linkable. This means that the anonymity of signatures produced before the revocation is compromised. In some cases that all signatures from an illegal person should be traced, the linkability is useful, as well as traceable signatures in [13]. However, the linkability is undesirable in most cases. In case a member leaves voluntarily, the anonymity of signatures before leaving should be ensured. This is the same in case a member's secret key is stolen. In this paper, author propose VLR group signature schemes from bilinear maps, which moreover satisfy the backward unlink ability. In the schemes, the concept of time intervals is adopted.

The jammer deliberately generates interfering transmissions that prevent communication within their reception range. As the network coverage area, e.g., along a highway, can be well-defined, at least locally, jamming is a low-effort exploit opportunity.

An attacker can relatively easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network. The correctness and timely receipt of application data is a major vulnerability. The rapid "contamination" of large portions of the vehicular network coverage area with false information where a single attacker forges and transmits false hazard warnings (e.g., ice formation on the pavement), which are taken up by all vehicles in both traffic streams. With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. Then, inferences on the drivers' personal data could be made, and thus violate her or his *privacy*2. The vulnerability lies in the periodic and frequent vehicular network traffic: safety and traffic management messages, context-aware data access (e.g., maps, ferryboat schedules), transaction-based communications (e.g., automated payments, car diagnostics), or other control messages (e.g., over-the-air registration with local highway authorities). In all such occasions, messages will include, by default, information (e.g., time, location, vehicle identifier, technical description, trip details) that could precisely identify the originating node(vehicle) as well as the drivers' actions and preferences. Beyond abuse of the communication protocols, the attacker may select to tinker with data (e.g., velocity, location, status of vehicle parts) at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler to replace or by-pass the real-time clock or the wiring of a sensor, rather than modifying the binary code implementation of the data collection and communication protocols. Any VC security architecture should achieve a trade-off between robustness and cost due to tamper-proof hardware.

A sample system architecture of a campus PCE is given. Generally, a PCE consists of three types of entities: mobile users, services and back end authentication servers, in addition to the underlying wired and wireless communication infrastructures. Note that wireless network access is itself a service. User

privacy should be protected not only from outsiders but also from network service providers. Our proposed access control scheme is designed to secure the interactions among these three types of entities as shown. More specifically, our scheme aims to provide anonymous mutual authentication between the mobile user and the service (e.g., wireless service access point for wireless network access service). It also provides the confidentiality and integrity protection for the communications between the mobile user and the service. Our scheme is based on two cryptographic techniques, blind signature and hash chain. A brief review of the two techniques is provided.

Blind signature scheme [16] is a variation of digital signature scheme in which the content of a message is disguised from its signer. Blind signature schemes can be implemented based on a number of well-known digital signature schemes, such as RSA [33]. To produce a signature on a message, a user first *blinds* the message with a *blinding function* f, typically by combining it with a random *blinding factor* k, and then forwards the blinded message to the signer. The signer signs the blinded message using a standard signing algorithm, say SA(m) which denotes the signature of A on m, and sends the result back to the user, who then unblinds it with an unblinding function g to obtain the signer's signature on the original message.

A Service-Agent-Based Roaming Architecture for WLAN/Cellular Integrated Networks Although user roaming is well defined in the cellular network through authentication, authorization, and accounting (AAA), it is still an open issue in the WLAN networks operated by multiple service providers. Many WISPs provide public WLAN Internet access at the hotspots using a network access server (NAS). The NAS allows only legitimate customers to use the service and provides intra domain roaming because the hotspots from one WISP share the same customer base. However, it lacks an architecture to provide inter domain roaming and MIP support. Currently, multiple accounts for those service providers are required for a user to use the service in corresponding network territories. Due to the manual interaction between the users and a log on Web page, seamless network service offering is not available. On the other hand, since the network structure of the cellular network is quite different (much more complex and expensive) from the WLAN hotspot, it is difficult to import the authentication scheme, used in the cellular network to the WLAN hotspot.

Protecting location privacy with personalized k-anonymity: Architecture and algorithms Advances in global positioning and wireless communication technologies create new opportunities for location based mobile applications, but they also create significant privacy risks. Although, with LBSs, mobile clients can obtain a wide variety of location-based information services, and businesses can extend their competitive edges in mobile commerce and ubiquitous service provisions, the extensive deployment of LBSs can open doors for adversaries to endanger the location privacy of mobile clients and to expose LBSs to significant vulnerabilities for abuse. A major privacy threat specific to LBS usage is the location privacy breaches represented by space or time correlated inference attacks. Such breaches take place when a party that is not trusted gets access to information that reveals the locations visited by the individual, as well as the times during which these visits took place. An adversary can utilize such location information to infer details about the private life of an individual such as their political affiliations, alternative lifestyles, or medical problems or the private businesses of an organization such as new business initiatives and partnerships. Consider a mobile client which receives a real-time traffic and roadside information service from an LBS provider. If a user submits her service request messages with raw position information, the privacy of the user can be compromised in several ways, assuming that the LBS providers are not trusted but semi honest. For instance, if the LBS provider has access to information that associates location with identity.

A flexible privacy enhanced location-based services system framework and practice:

The architecture author propose architecture includes the basic functions required to provide an LBS and does not imply a physical implementation or deployment. The user device may generate, or assist in generating, its own location information, and may receive the location of other end users as part of a service. To be able to correctly receive the location information of a client, the recipient must be a member in a location information group controlled by the client. The location information group defines the members that receive location information at a particular granularity. Access to the location information by a

group is controlled through the distribution of keys that decrypt the location information.

The architecture supports a range of control by the end user. In the most highly controlled case, the end user generates their own location information and encrypts it, and distributes keys directly to the other members of the location information group using a protocol like Diffe-Hellman, or even running a group key management protocol as described later in this paper. This solution is feasible for small information groups. For larger groups, the end user may form a trust relationship with a server in the network. Depending on the level of trust, the server(s) may have more or less access to the location information. At one level, the user may allow the network to store and distribute its location information in an encrypted form and still manage key distribution itself.

BAT: A Robust Signature Scheme for Vehicular Networks Using Binary Authentication Tree Application Scenario Model Author consider the representative Vehicleto-Infrastructure communications architecture, which includes:

- RSU: A RSU serves as a gateway connecting the vehicles within its transmission range to the Internet.
- Vehicles: A vehicle periodically exchanges messages with the RSU within its range. Each vehicle is equipped with sensing and processing units, OBUs (On-BoardUnits).
- TA (Trusted Authority): The TA server, as the key distribution center, is responsible for generating and assigning related parameters for the vehicles and RSUs, and identifying a malicious identity for any dispute events.
- SP (Service Provider): The SP or Application Server is responsible for collecting the traffic related information such as location, traffic accidents, and other important information from RSUs, and making further analysis and giving response to RSUs.

Protecting Location Privacy in Sensor Networks against a Global Eavesdropper In this section, author present two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal level of location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical tradeoffs between privacy, communication overhead, and latency. Sensor networks can support a wide range of applications. Different applications have different requirements that may affect the usage of the periodic collection method in real-world scenarios. Example of these requirements includes the latency of a real event being reported to the sink and the network lifetime. There is a trade-off between energy consumption and latency depending on the value. Since the setting of the value determines the amount of wireless communication and corresponding energy consumption in the network, it also determines how long the sensors' batteries will last.

Privacy-Preserving Universal Authentication Protocol for Wireless Communications Author assume that the attacker has total control over all communication channels among the user, foreign server and home server. That is, the attacker may intercept, insert, delete, or modify any message in the channels. Particularly, author consider four major types of threats to user authentication, namely, message en route threat, false mobile user threat, DoS attack and deposit-case attack [4]. The message en route threat includes that an attacker relays and/or redirects messages. The false mobile user threat includes the case where an attacker could impersonate a foreign/home server, as well as the case where mobile users under the control of an attacker collude. DoS attack refers to the overwhelming service requests from attackers in the purpose of blocking services from genuine mobile users. In deposit-case attack, the user is honest while there is a malicious server , who will make the foreign server to believe that the home server of the user is without being detected by the user nor its home server. This paper makes two main contributions: (1) Author show some security weaknesses of current user authentication protocols in wireless communications. (2) Author proposes a privacy preserving universal authentication protocol called Priauth. By introducing Verifier-Local Revocation Group Signature with Backward Un linkability (VLR-GS-BU), it can satisfy all requirements described. Analysis and Improvement of a Secure and Efficient Handover Authentication for Wireless Networks

There has been a lot of research focusing on handover authentication, and many interesting protocols

have been proposed in recent years [1]– [12]. However, not every proposal is suitable for mobile networks, because an MN is generally constrained in terms of power and processing capability while the IEEE is discussing a 20-ms limit on handover authentication time. Furthermore, security and privacy become serious concerns for handover service while mobile networks are vulnerable to attacks due to the broadcast nature of the wireless communication environment. Quite recently, He *et al.* proposed a novel handover authentication protocol named *PairHand* [13]. PairHand is computation- and communication-efficient because, for mutual authentication and key establishment, it only requires two handshakes between an MN and an AP, and does not need to transmit or verify any certificate as in traditional public key cryptosystems. On the contrary, other protocols without involving communication with AS require at least three handshakes between an MN and an AP while those protocols involving communication with AS require at least four handshakes among the three entities.

3. SYSTEM MODEL

Due to their natural mobility and scalability, wireless networks are always preferred since the rest day of their creation. Due to the improved technology and reduced costs, wireless networks have increase much more preferences over wired networks in the past a lot of decades. By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility.

However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi hop. In a single-hop network, all nodes within the same radio range communicate directly with each other.

On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflict, and medical emergency situations.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

- Network Topology
- IDS (Intrusion Detection System) in MANETs
- Ack and S-Ack Scheme
- MRA and Digital Signature Scheme
- Routing Overhead

3.1 Network Topology

In our first module, we have to establish the Network. In this network, can have created the N nodes. These nodes are used to communicating each other indirectly

to through the neighbor nodes. Using multicast socket, all nodes are used to detect the neighbor nodes.

3.2 Ids In MANET'S

The assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches.

3.3 Ack and S-Ack Scheme

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in Enhanced Adaptive Acknowledgement (EAACK), aiming to reduce network overhead when no network misbehavior is detected. S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

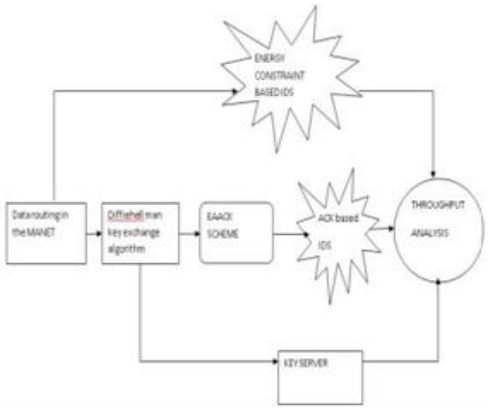
3.4 MRA AND DIGITAL SIGNATURE SCHEME

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. The Digital Signature requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. The goal is to find the most optimal solution for using digital signature in MANETs.

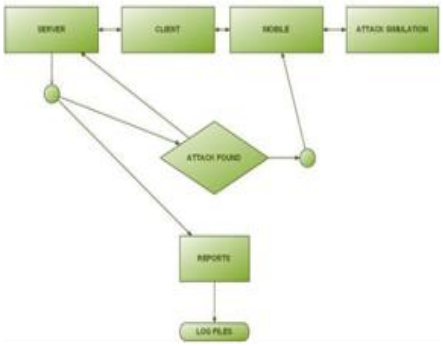
3.5 Routing Overhead

The RO defines the ratio of the amount of routing-related transmissions during the simulation; the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

4. ARCHITECTURE DIAGRAM



5. DATA FLOW DIAGRAM



6. CONCLUSION

We focus on the multiple data set scenarios, and divide the data set in the database into multiple security domains that greatly reduces the key management complexity. We propose a novel data-centric framework and suite of mechanisms for data access control for information, we leverage attribute based encryption (ABE) technique to encrypt each data. We propose a novel data-centric framework and a suite of Mechanisms for data access control stored in semi-trusted servers. To achieve fine-grained and scalable data access control for files.

To break through the limitations of traditional data mining methods, we have studied heterogeneous information discovery and mining in complex inline data, mining in data streams, multigranularity knowledge discovery from massive multisource data, distribution regularities of massive knowledge, quality fusion of massive knowledge.

REFERENCES

[1] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps," in Proc. ASIACRYPT, Chennai, India, 2005, pp. 533–548.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.

[3] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," IEEE Trans. Veh. Technol., vol. 55, no.4, pp. 1373– 1384, Jul. 2006.

[4] M. Shi, H. Rutagemwa, X. Shen, J. W. Mark, and A. Saleh, "A service-agent-based roaming architecture for WLAN/cellular integrated networks,"IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 3168–3181, Sept. 2007.

[5] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

[6] Y. Sun, T. La Porta, and P. Kermani, "A flexible privacy enhanced location-based services system framework and practice," IEEE Trans. Mobile Comput., vol. 8, no. 3, pp. 304–321, Mar. 2009.

[7] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Trans. Wireless Commun., vol. 8, no. 4, pp. 1974–1983, Apr.2009.

[8] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," IEEE Trans. Mobile Comput., vol. 11, no. 2, pp. 320–336, Feb. 2011.

[9] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431 436, Feb.2011.

[10] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," IEEE Commun. Lett., vol. 16, no. 8, pp. 1270 1273, Aug.2012