www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks

[1]Mrs.C.Navamani MCA., M.Phil., M.E., Assistant Professor,
[2]Mr.A.Dhanasekar Final MCA,
Department of MCA, Nandha Engineering College(Autonomous),Erode-52.
E-Mail ID: navamanimca@gmail.com, dhanaxpress@gmail.com

***Abstract*- Over the past two decades, vehicular networks have been emerging as a cornerstone of the next-generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. In vehicular networks, moving vehicles are enabled to communicate with each other via inter-vehicle communications as well as with road-side units (RSUs) in vicinity via roadside-to-vehicle communications. In urban vehicular networks where the privacy, especially the location privacy of vehicles should be guaranteed, vehicles need to be verified in an anonymous manner. In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable.**

Index Terms:*, *Inter-Vehicle Communication (IVC)*, *Intelligent Transportation Systems (ITS)*,Road-side units (RSUs), *VANET is a technology.

I.INTRODUCTION

A Vehicular Ad-Hoc Network, or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

In VANET, or Intelligent Vehicular Ad-Hoc Networking, defines an Intelligent way of using Vehicular Networking. InVANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well as methods to track the automotive vehicles.

In VANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.

Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).

As envisioned in ITS, vehicles communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC). The optimal goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities. The Sybil attack in computer security is an attack wherein a reputation system is subverted by

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder. The name was suggested in or before 2002 by Brian Zill at Microsoft Research. The term "pseudospoofing" had previously been coined by L. Detweiler on the Cypherpunks mailing list and used in the literature on peer-to-peer systems for the same class of attacks prior to 2002, but this term did not gain as much influence as "Sybil attack".

A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. So the title is chosen to find and prevent the sybil attack detection in vehicular networks.

A. Objectives

The following are the objectives of the project

- To find and eliminate Sybil trajectories
- Location privacy of vehicles is preserved
- To fast detect the corruption of an RSU
- linkable signer-ambiguous signature schemes
- Computation overhead for signature verification and the communication overhead can be reduced.

II.RELATED WORKS

Over the past two decades, vehicular networks have been emerging as a cornerstone of the next-generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. In vehicular networks, moving vehicles are enabled to communicate with each other via intervehicle communications as well as with road-side units (RSUs) in vicinity via roadside-to-vehicle communications.

In urban vehicular networks where the privacy, especially the location privacy of vehicles should be guaranteed vehicles need to be verified in an anonymous manner. A wide spectrum of applications in such a network relies on collaboration and information aggregation among participating vehicles.

Without identities of participants, such applications are vulnerable to the Sybil attack where a malicious vehicle masquerades as multiple identities overwhelmingly influencing the result. The consequence of Sybil attack happening in vehicular networks can be vital. For example, in safety-related applications such as hazard warning, collision avoidance, and passing assistance, biased results caused by a Sybil attack can lead to severe car accidents. Therefore, it is of great importance to detect Sybil attacks from the very beginning of their happening.

Detecting Sybil attacks in urban vehicular networks, however, is very challenging. First, vehicles are anonymous. There are no chains of trust linking claimed identities to real vehicles. Second, location privacy of vehicles is of great concern. Location information of vehicles can be very confidential. For example, it can be inferred that the driver of a vehicle may be sick from knowing the vehicle is parking at a hospital. It is inhibitive to enforce a one-to-one correspondence between claimed identities to real vehicles by verifying the physical presence of a vehicle at a particular place and time.

Third, conversations between vehicles are very short. Due to high mobility of vehicles, a moving vehicle can have only several seconds to communicate with another occasionally encountered vehicle. It is difficult to establish certain trustworthiness among communicating vehicles in such a short time. This makes it easy for a malicious vehicle to generate a hostile identity but very hard for others to validate.

Furthermore, short conversations among vehicles call for online Sybil attack detection. The detection scheme fails if a Sybil attack is detected after the attack has terminated. To eliminate the threat of Sybil attacks, it is straightforward to explicitly bind a distinct authorized identity (e.g., PKI-based signatures) to each vehicle so that each participating vehicle can represent itself only once during all communications.

Using explicit identities of vehicles has the potential to completely avoid Sybil attacks but violates the anonymity concern in urban vehicular networks. As an alternative scheme, resource testing can be conducted to differentiate between malicious and normal vehicles, where the judgment is made whether a number of identities possess fewer resources (e.g., computational and storage ability) than would be expected if they were distinct. This scheme fails in heterogeneous environments where malicious vehicles can easily have more resources than normal ones.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

www.ijiarec.com

Considering the fact that a vehicle can present itself at only one location at a time, localization techniques or other schemes like the Global Positioning System (GPS) aiming to provide location information of vehicles can be exploited to detect hostile identities.

However, these schemes often fail in complicated urban settings (e.g., bad GPS signals due to urban canyons, inaccurate localizations due to highly dynamic wireless signal quality). Recently, two group-signature-based schemes have been proposed, where a message received from multiple distinct vehicles is considered to be trustworthy.

Using group signatures can provide anonymity of vehicles and suppress Sybil attacks by restraining duplicated signatures signed by the same vehicles. One practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to a biased or no final decision. As a result, there is no existing successful solution, to tackling the online Sybil attack detection problem in urban vehicular networks.

While it was first described and formalized by Douceur the Sybil attack has been a severe and pervasive problem in many forms. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a disproportionately large influence. In the literature, there have been many different approaches proposed to detect or mitigate the attack.

Many studies have followed Douceur's approach, focusing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, for example, P2P systems sensor networks and mobile ad hoc networks. Although deploying trusted certificates is the only approach that has the potential to completely eliminate Sybil attacks, it also violates both anonymity and location privacy of entities.

In addition, most of these schemes rely on a centralized authority that must ensure each entity is assigned exactly one identity. Moreover, it is possible for an attacker to violate the assumption, getting more than one identities. This mechanism also has the problem of key revocation which is challenging, particularly in wireless mobile networks.

Another category of Sybil attack detection schemes is based on resource testing. The goal of resource testing is to determine if a number of identities possess fewer resources than would be expected if they were independent. The resources being tested can be computing ability, storage ability, and network bandwidth, as well as IP addresses. These schemes assume that entities have homogeneous hardware configurations.

In vehicular networks, this assumption cannot hold since malicious vehicles can easily have more powerful resources than the normal vehicles. SybilGuard is an interesting scheme studying the social network among entities. In this scheme, human-established real-world trust relationship among users is used for detecting Sybil attacks. Since even the attacker can generate as many as Sybil identities, building relationship between honest users and Sybil identities is much harder.

Thus, there exists a small "cut" on the graph of trust relationship between the forged identities and the real ones. However, this scheme cannot be used in vehicular networks, since it is very challenging to establish such trust relationship among vehicles. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles.

To exploit the fact that one single vehicle cannot present at multiple locations at the same time, Bouassida et al. have proposed a detection mechanism utilizing localization technique based on Received Signal Strength Indication (RSSI). In this scheme, by successively measuring the RSSI variations, the relative locations among vehicles in vicinity can be estimated. Identities with the same estimated locations are considered as Sybil vehicles.

In practice, the complicated outdoor environments can dramatically affect the wireless signal propagation so that RSSI measurements are highly time variant even measured at the same location. Xiao et al.have proposed a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements taken at other participating vehicles. In addition to the inaccuracy of RSSI measurements, this scheme also needs all neighboring vehicles to collaborate which may suffer a Sybil attack against the detection scheme itself. Zhou et al. have proposed a privacy-preserving Sybil attack detection scheme using pseudonyms. In the scheme, the trust authority distributes a number of pseudonyms for each vehicle.

Abused pseudonyms can be detected by RSUs. Since RSUs are heavily involved in the detection process, this scheme requires the full coverage of RSUs in the field. It is infeasible in practice due to the prohibitive cost. Furthermore, in such a scheme, vehicles should managed by a centralized trusted

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

www.ijiarec.com

center. Each time RSU detects suspicious pseudonyms, it should send all the pseudonyms to the trust center for further decision, which makes the trust center be the bottleneck of the detection.

Recently, two group-signature-based schemes have been proposed, ensuring that a verifier vehicle can identify those trustworthy messages from messages sent from neighboring vehicles. A message sent from a neighboring vehicle is said to be trustworthy if the content of the message is identical with at least a certain number of messages sent from other neighboring vehicles.

To suppress duplicated messages from the same vehicle, particular group signature schemes are adopted for vehicles to sign on messages so that the anonymity of each vehicle can be achieved. Meanwhile, if a vehicle generates two signatures on the same message, these two signatures can be recognized by the verifier vehicle.

One practical issue of these schemes is that they cannot handle similar but different messages. It is often the case that multiple vehicles observing the same driving environment will generate different messages with very similar semantics. In this case, the resolved trustworthy messages might be a minority of all observations which results in a biased or no final decision.

The most relevant work to Footprint is the Sybil attack detection schemes proposed in. In these schemes, a number of location information reports about a vehicle are required for identification. In, an RSU periodically broadcasts an authorized time stamp to vehicles in its vicinity as the proof of appearance at this location. Vehicles collect these authorized time stamps which can be used for future identity verification. In, trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification.

However, these schemes did not take location privacy into consideration since RSUs use long-term identities to generate signatures. As a result, the location information of a vehicle can be inferred from the RSU signatures it collects.

In Footprint, authorized messages issued from RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed, and temporarily linkable which means using a single trajectory for long-term identification of a vehicle is prohibited. Therefore, the privacy of location information and identity of vehicles are preserved in Footprint.

III.SYSTEM METHODOLOGY

The main objective for designing the system is Sybil attack detection in Vehicle ad-hoc network. The network creation is the beginning process of the application. The proposed a novel Sybil attack detection scheme Footprint, using the trajectories of vehicles for identification while still preserving the anonymity and location privacy of vehicles. Specifically, in Footprint, when a vehicle encounters an RSU, upon request, the RSU issues an authorized message for this vehicle as the proof of its presence at this RSU and time. Intuitively, authorized messages can be utilized to identify vehicles since vehicles located at different areas can get different authorized messages.

- The Vehicle ad-hoc network creation in the specified geographical area.
- Deployment of Road Side Unit (RSU) and apply RSA algorithm to generate private and public key of the RSU.
- Create Trajectory between one Road Side Unit (RSU) and neighbor RSU along with specified distance.
- Initializing Vehicle and apply RSA algorithm to create private and public key of the On Board Unit.
- Entry the time of the traversed details are stored in RSU and OBU
- Partial signature created for new vehicles and details of RSU and OBU is Encrypted using RSA algorithm.
- Partial signature is verified to evaluate the security level.
- Full signature is created for traversed vehicle.
- Full signature verified to evaluate the security level.
- Detection of Sybil attack and Failure RSU.
- Analyze the results.

A. System Architecture

In vehicular networks, a moving vehicle can communicate with other neighboring vehicles or RSUs via inter-vehicle communications and roadside-to-vehicle communications. In general, Footprint integrates three elegant techniques namely, infrastructure construction, location-hidden trajectory generation, and Sybil attack detection.

More specifically it is used to adopt an incremental methodology to deploy RSUs. In the end, a limited number of available RSUs can achieve the

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

www.ijiarec.com

maximum service coverage in terms of served traffic amount as well as good fairness in terms of geographical distribution.

After the deployment of RSUs, a vehicle can require authorized messages from each RSU it passes by as a proof of its presence. In this Foot print authenticated m scheme for RSUs to issue authorized messages for vehicles. Such authorized messages are location hidden which refers to that RSU signatures is signer ambiguous and the authorized messages are temporarily linkable.

Furthermore, a set of consecutive authorized messages issued for a vehicle are tightly chained together to form a location-hidden trajectory of the vehicle, which will be utilized for identifying this vehicle in future conversations.

During a conversation which is initialized by a vehicle or an RSU, called a conversation holder, a participating vehicle should provide its trajectory for verification. With the trajectories sent from all participating vehicles, the conversation holder can conduct online Sybil attack detection according to the similarity relationship between each pair of trajectories. Among all trajectories, Sybil trajectories forged from the same attacker are bound to gather within the same "community." By treating each "community" as one single vehicle, Sybil trajectories can be largely eliminated.

The architecture of the system model, which consists of three interactive components:

- Road Side Unit (RSU):
- On-board units (OBUs):
- Trust authority (TA):

Road side unit (RSU): The RSU can be deployed at intersections or any area of interest (e.g., bus stations and parking lot entrances). A typical RSU also functions as a wireless AP (e.g., IEEE 802.11x) which provides wireless access to users within its coverage. RSUs are interconnected (e.g., by a dedicated network or through the Internet via cheap ADSL connections) forming a RSU backbone network.

On-board units (OBUs): The OBU are installed on vehicles. A typical OBU can equip with a cheap GPS receiver and a short-range wireless communication module (e.g., DSRC IEEE 802.11p). A vehicle equipped with an OBU can communicate with an RSU or with other vehicles in vicinity via wireless connections. For simplicity, we simply refer to a vehicle as a vehicle equipped with an OBU in the rest of this paper. A vehicle can be malicious if it is an attacker or compromised by an attacker.

*Trust Authority (Ta):*The TA is responsible for the system initialization and RSU management. The TA is also connected to the RSU backbone network. Note that the TA does not serve vehicles for any certification purpose in Footprint. A vehicle can claim as many arbitrary identities as it needs.

B. Deployment Of Road Side Unit(Rsu)

In Footprint, vehicles require authorized messages issued from RSUs to form trajectories, which should be statically installed as the infrastructure. When considering the deployment of RSUs, two practical questions are essential. A simple solution is to deploy RSUs at all intersections. This can result fine trajectories with a sufficient number of authorized messages which will facilitate the recognition of a vehicle.

However, deploying such a huge number of RSUs in one time is prohibitive due to the high cost. In contrast, we take an incremental deployment strategy in Footprint, considering the tradeoff between minimizing the number of RSUs and maximizing the coverage of traffic. Specifically, in the early developing stage with a limited number of RSUs, an intersection is chosen if it satisfies two requirements:

- it is geographically at least certain distance far away from all other RSU.
- it has the maximum traffic volume among all rest intersections without RSUs.

The reason for requiring two RSUs at least certain distance far away is to avoid uneven deployment where RSUs are consecutively deployed along a high-traffic-volume road. As more RSUs are available to install, a smaller distance can be used to deploy RSUs according to the above strategy. Given an RSU deployment, two RSUs are said to be neighbors if there exists a path in the underlying road networks along which no other RSUs are installed.

C. Location-hidden authorized message generation

In order to be location hidden, authorized messages issued for vehicles from an RSU should possess two properties, i.e., signer ambiguous and temporarily linkable.The temporarily linkable property requires two authorized messages are recognizable if and only if they are generated by the same RSU within the same given period of time.

In this signature scheme, to define an event as

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

a period of time within which two signatures issued from the same RSU are linkable. Thus, an RSU signature consists of three parts:

- RSU ID and its Public Key
- Vehicle Id and its Private Key
- Entry time as message

The ps(Partial Signature) is a proof that the signature on the message M is legitimate. The public key of road side unit and private key of on board unit fixed-size bit string derived by a secure cryptographic hash function on an event (i.e., a period of time). The message is generated based on the time and the public key of an RSU. With time variant link tags, the RSU signatures can meet the temporarily linkable requirement.

In Footprint, when a vehicle approaches an RSU, it demands a time stamp as Message (M) from RSU, using a public key of RSU and private Key of vehicle Id of temporarily generated key pair. Upon request, RSU generates a message M for Vehicle, which includes RSU public, and a time stamp indicating the time when this message is generated. Then, RSU signs on the message M and sends M together with the signature.

D. Rsa encryption algorithm

The security of a cryptographic system should not be based on the privacy of its implementation. It should be based on the strength of its underlying mathematical cryptographic algorithm. An algorithm is a procedure or formula. The algorithm is used for encrypting, decrypting bytes and text with public and private keys using asymmetric algorithm RSA. Also enables generate keys. RSA is used for encrypting smaller amount of data. Use Get Max Data Length method to check maximum data length for specified key size.

E. key generation

- Choose two large random prime numbers P and Q of similar length. Generate two different large odd prime numbers, called P and Q, of about the same size where P is greater than Q that when multiplied together give a product that can be represented by the required bit length you have chosen, e.g. 1024 bits.
- Compute N = P x Q. N is the modulus for both the Public and Private keys.
- PSI = (P-1)(Q-1) , PSI is also called the Euler's totient function.
- Choose an integer E, such that 1 < E < PSI, making sure that E and PSI are co-
- prime. E is the Public key exponent.
- Calculate $D = E^{-1} (\text{mod PSI})$, normally using Extended Euclidean algorithm. D is the Private key exponent.

When representing the plain-text to plain-text octets in order to secure the message more thoroughly it is usual to add padding characters to make it less susceptible to certain types of attack. After all that has been accomplished you have public and private keys ready for encryption which are then stored as base-64 numbers.

F. Encryption

- Convert the data bytes to be encrypted, to a large integer called PlainText.
- $\text{CipherText} = \text{PlainText}^{E} (\text{mod N})$
- Convert the integer, CipherText to a byte array, which is the result of the encryption operation.

G. Decryption

- Convert encrypted data bytes to a large integer called Cipher Text.
- $\text{Plain Text} = \text{Cipher Text}^{D} (\text{mod N})$
- Convert the integer, Plain Text to a byte array, which is the result of the decryption operation.

H. Other considerations

1) As its clear that exponents are very large, as a result the large integers will easily overflow the normal 32 bit 'int' and 64 bit 'long'. To overcome this problem, we require to use a Big Integer library which can handle arbitrarily large numbers. In this case I used the Big Integer library provided with the .NET Framework (System. Numerics. BigInteger).

2) The conversion from Byte array to integer and vice-versa are done in a specific format.

In cryptography, everything starts with data that can be read without any extra effort referred to as "plain-text". The method of converting plain-text into unreadable gibberish called “cipher-text” is encryption. The process of reverting this gibberish back into the original plain-text is called decryption. Simply stated, cryptography is the science of using mathematics to scramble and descramble information. Cryptography allows the storage and transmission of sensitive material so that it can only be read by the intended recipient.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

Public key cryptography utilizes a public key for encryption as well as a corresponding private key for decryption. Because it uses two differing keys, it is sometimes called asymmetric cryptography. Asymmetric means unbalanced or different. While the public and private keys are mathematically related, it is computationally infeasible to deduce the private key from the public key, which requires factoring large prime numbers, without massive amounts of computing power. The primary advantage of public key cryptography is that it allows people who have no preexisting arrangement with you to exchange data securely.

I. Message verification

As the proof that a vehicle (Vi) was present near certain RSU (Rk) at certain time, an authorized message issued for Vi can be verified by any entity (e.g., a vehicle or an RSU) in the system. In the case that an entity needs to verify Vi, Vi will sign on an authorized message (M) generated by RSU (Rk) using public key and then send to the vehicle. The message verification process consists of following steps:

- Check the Vehicle Id
- Check the private key of RSU (Rk)
- Check the public key of Vehicle (Vi)
- Analyze the Entry time
- Analyze the message as partial signature or Full Signature creation
- Verify that the message was signed by legitimate previous RSU

IV.CONCLUSION

A Sybil attack detection scheme named Footprint is developed for urban vehicular networks. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories. The Footprint design can be incrementally implemented in a large city. It is also demonstrated by both analysis and extensive trace-driven simulations that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings (above 98 percent detection rate).

With the proposed detection mechanism having much space to extend, the future work is to continue to work on several directions. First, in Footprint, it is assumed that all RSUs are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories (e.g., by inserting link tags of other RSUs into a forged trajectory).

In that case, Footprint cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by itself nor forge link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system. In future work, the scenario where a small fraction of RSUs are compromised will be considered. The cost-efficient techniques can be developed to fast detect the corruption of an RSU. Second, it will delve into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

V. FUTURE ENHANCEMENTS

Last, the future work can validate the design and study its performance under real-complex environments. Improvements will be made based on the realistic studies before it comes to be deployed in large-scale systems.

REFERENCES

[1]Y.Sun,R.Lu,X.Lin,X.Shen,andJ.Su,"AnEfficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[2] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.

[3] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp. 251-260, Mar. 2002.

[4] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular Content Delivery Using WiFi," Proc. MOBICOM '08, pp. 199-210,Sept. 2008.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Symp. Operating Systems Design and Implementation (OSDI '02), pp. 299-314, Dec. 2002.

[6] B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," Technical Report SRI-SDL-04-02, SRI Int'l, Apr. 2002.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

www.ijiarec.com

'04), pp. 259-268, Apr. 2004.

[8] S. Capkun, L. Buttya'n, and J. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[9] C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," Proc. Securecomm and Workshop, pp. 1-11, Aug. 2006.

[10] N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. Sixth IEEE Int'l Conf. Peer-to-Peer Computing (P2P '06), pp. 171-176, Oct. 2006.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations,

www.ijiarec.com