ISSN 2278-

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.5, Pages : 451- 455 (2014)
*Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh*

# A Framework for Attaining Uncertainty and Traceability in WMN

**[1]G.Vinay Reddy**, **[2]V.VisweswaraRao**
[1]Final M.Tech Student, [2]Assistant professor
[1,2]Dept of Computer Science and Engineering
[1,2]Pydah College of Engineering, Visakhapatnam, AP, India

Abstract: Anomaly detection is one of the interesting research issues in network security.Identification of anonymous behavior is a complex task to analyze. Anonymity achieves security for users to attack free network services. The situations related to anonymity have been strongly studied in payment based systems such as online cash payment and node to node systems and a less effort has been included to wireless mesh networks (WMNs). In other case the network authority requires conditional anonymity such asmaliciousproperties in the network channel remains traceable. In our work we propose architecture to safeguardunreserved anonymity for authenticated and trusted users and traceability of malicious users for network authentications in WMNs. The proposed architecture works to resolve the disputes between the anonymity and traceability objectives. Quick analysis on security and efficiency is absorbed and testing the efficiency of the proposed architecture.

## INTRODUCTION

Generally wireless sensor networks are depends on applications and mainly designed for real time analyzing the low level data environments. Many wireless networks include military commands, organizational quality control and monitoring of traffic control etc. Most of the network is hosted in adverse environments with smart opposition. So the security is main issue [1][2].

Consider an example in battle applications there is major need to maintain secrecy of location and destroying of the network. It is not frequent but mainly depends on security. These include the following as shown below:

1. In military applications, to preserve the details of locations and data confidentiality from unauthorized users.
2. In chemical and Hazardous environment , to raise false alarm and for intra signal transmission
3. In home and health centers, for transmission of information regarding emergencyservices.

Although various traditional approach of anomaly detection and prevention techniques available to identify anomaly, they are not accurate while analyzing the behavior of the samples. Some of the techniques are as follows

- Statistical based techniques
- Cluster based techniques
- Trust measure based techniques
- Data rating based techniques
- Classification based techniques

Every approach has its own individual advantages and disadvantages based on context or on what data they are applied for anomaly detection. In trust based anomaly detection mechanism destination node completely depends on the centralized server trust metrics instead of individual analysis [3][5].

Cluster based approaches groups the similar type of anonyms objects based on similar features of misbehaved user but it cannot analyze new anomaly behavior in both clustering and classification approaches[4].

## RELATED WORK

There are many types of network routing techniques but in those we will discuss about two routing techniques such as onion routing and selfish mac layer malicious behaviors.

Coming to onion routing, it is topology for protected communication in public networks. It provides the secured connections and they are mainly defended on malicious attacks.In this connections are bidirectional and it is very similar to real time networks and it can be used in any network connection [6][7].

These routing connections are acts as verifiers and auditors in the network. And the same process continued in the establishment of the connections of the network. These are mainly used in lab networks and communication websites [8][10].

When coming to selfish mac layer misbehavior it uses decentralized connection method for distributing the wireless network. In these networks the environment is selfish hosts that get distorted result to share. Consider an example that mainly needs competing for access control to network channel to wait and dynamically selected particular range before initializing the transmission. Selfish hosts wait for some time back off intervals thanall-behaved hosts, thereby obtaining an unfair advantage.

Our proposed architecture has major features such as:

1. Framework for secure and efficiency of the network with traceability

ISSN 2278-

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.5, Pages : 451- 455 (2014)
*Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh*

2. Blinding technique with user authenticating at the access point.
3. In this architecture we adopted hierarchical identity-based cryptography for reducing the authentication of domain parameter certification [10].

## PROPOSED WORK

In this paper we are proposing an efficient and empirical model in wireless sensor networks and it consists of mesh routers (MRs) and gateways (GWs) are connected each other by ordinary wireless links. Mesh routers and gateways provide as the access control points of the WMN and the final resorts to the web respectively. The hospitaland residential buildings are the objects of individual WMN domains registering to the web services from service providersshown as Internet cloud in Fig. Every WMN domain or trust domain is maintained by a domain manager that gives as a trusted authority for example the global server of a campus WMN. The trusted authority and respected gateways are inter-connected by high speed wired or wireless connects which is displayed as solid and bold dashed lines.

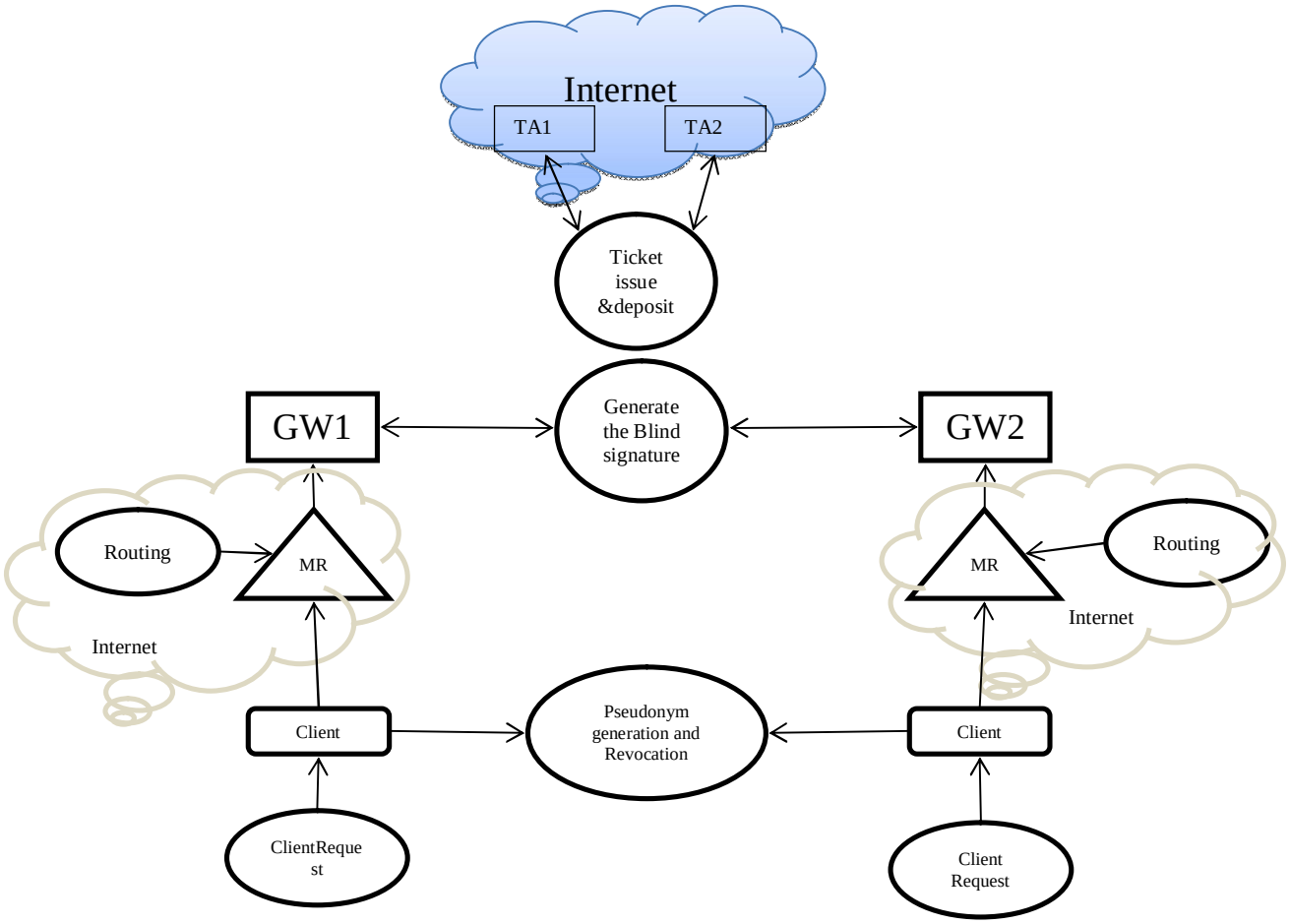


Fig1 : Proposed Architecture

Trusted authorities and gate ways are considered to capable of managing computations of intensive tasks. Other than this they are considered to be secured in private places and cannot be flexible compromised due to their main roles in the WMN. The WMNs focused here are those where the trusted and it provides free Internet access but requires the clients (CLs) to be authorized and registered members normally for a long term use in WMNs.

### 1. Client & Trusted Node Deployments

The trusted authority is trusted memberwithin the WMN domain. There are indirect trust between the client and the gateway or network router. We use IBC for authentication and secure data exchange and conversation of both and during network access control inside a trust domain (i.e., intra domain). We consider the shared keys and secure network channels between objects at the backbone and it will consider the validation process and key generationwhen the

ISSN 2278-

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.5, Pages : 451- 455 (2014)
*Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh*

network access of the clients. The client gives his ID upon registration at the TA which assigns a private key related with the client's ID.

The client chooses a distinct account number calculated by a dynamically chosen secret number $u_1$. The account number is saved with the client's ID at the trusted authority. The trusted authority also assigns an ID or private key pair to each gateway and network router in its trust domain before hosting. The benefits of this trust relationship with the trusted authority system from the direct authentication of the clients moving among gateways or network routers in the similar domain which decreases network access latency and communication cost is expected to be exiting in future WMNs due to the large user population and high mobility. The domain starting process of the hierarchical IBC is particularly the root public key generator (PKG) at level 0 in the HT performs the following domain initialization algorithm when the network is boot-strapped, where $P_0$ is a generator of $G_1$.

**2.Ticked Issuance And Deposit Process**

Ticket issuance happens when the client initially tried to access the network or when all previously issued tickets are depleted. The client required to reveal his or her real ID to the trusted authority in order to obtain a ticket since the TA has to issue the authenticity of this client. The TA should not able to link the ticket it issued to the clients real details of identity. The client employs some blinding technique to transform the ticket to be un-linkable to particular execution of the ticket generation algorithm while managing the verifiability of the ticket. The ticket generation algorithm which can be restrictive partially blind signature scheme which takes as input the client's and TA's secret numbers. The common agreement c and some public parameters and generates a valid ticket = {TN, W, C, (U', V', X')} get the result, where TN is the distinct serial number of the ticket that can be computed from the client's account number

This information is abstracted at the TA by processing the fraud detection based on the ticket records generated by gateways that have serviced this client. By placing the malicious information in c, the TA informs gateways about the client's past malicious behavior when the ticket is deposited. A valid ticket the client may be deposit it at any time the network service is desired before the ticket time out using the ticket deposit protocol shown in architecture. Our methodlimits the ticket to be deposited only once at the first encountered gateway that provides network access services to the client based onval before exp. The ticket is deemed valid if both the signature verification and the above equality check is successful. The gateway (DGW)where the ticket is basically depositand itcreates a signature on the client pseudonym.The DGW's ID, and the respectivemis$_b$ and exp values abstracted from c. the trusted authority may bereduce the value of the issued tickets or decrease the frequency of approving the client's ticket requests based on the misbehavior level indicated in mis$_b$.

**3. Generate Pseudonym and Refraction Process**

The use of pseudonyms has shown in the ticket-based protocols. This section copies with the pseudonym generation technique and the related refraction issue. The pseudonym is used to replace the real ID in the authenticationwhich is essential for both anonymous network access and location privacy. In the intra-domain authentication in our system and the client creates his own pseudonym by choosing a secret value $2 and calculating the pseudonym PSCL {H1, IDCL, and P}. The respective private key can be defined as g=CL, CLH1, IDCL, PSCL a batch of pseudonyms are assigned to each client by trusted authority the self-generation processdecreases the communication expensive in the system. The client is able to update his pseudonyms to modify the anonymity by using this non-expensive method. As a last note on the self-generation algorithm, it would render the pseudonym refraction impossible by using the pseudonym alone.

The reason is adversary who has compromised a client can generate valid pseudonym or key pairs are only known to the adversary by running the self-generation algorithm. This pseudonym self-generation technique is appropriate in our system because the pseudonym refraction can be realized via revoking the associated ticket since the pseudonym is active only when its associated ticket is actively in use. In addition to the ticket-related operations the TA will be needed to create and update the pool of pseudonyms for the client and to distribute the refraction list for revoking all effective pseudonyms in the active pool during a particular period which induces convincingly higher signaling expensive. The TA will also be able to define the real identity corresponding to the assigned pseudonyms, which destroys the anonymity for honest clients.

**4. Blind Signature Generations**

A blind signature scheme allows a receiver to get a signature on a message such as both the message and the resulting signature remain unknown to the signer. We refer the readers to for a formal definition of a blind signature scheme which should bear the properties of verifiability, un-link-ability, and un-forge-ability the first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information.

Restrictive partially blind signature schemes were derived from the aforementioned work. They are necessarily blind signature schemes with restrictiveness and partial blindness properties. In the restrictive partially blind signature schemes that serve as a building block for our architecture, the two key concepts, namely restrictiveness and partial blindness A signature scheme is partially blind if, for all probabilistic polynomial-time algorithm A, A wins the game in the signature issuing

ISSN 2278-

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.5, Pages : 451- 455 (2014)
*Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh*

## 5. Fraud Detection & Ticket Refraction Process

Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple -deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA.

These are two types of fraud share a common feature and that is a similar ticket is deposited more than once such that our one-time deposit rule is violated. This is what the limited of the blind signature algorithm takes response on revealing the real identity of the misbehaving client. When TA findsredundant deposits using the ticket records reported by gateways, the TA will have the view of at least two various challenges from gateways and two respectivegroup of results from the same client. By evaluating the equation sets based on these challenges and responses and the TA is able to get the identity information encrypted in the message and then the real identity of the misbehaving client.

1. Refraction of novel tickets: The client may save a number of unused ticketsas declared previously. When revoking these tickets that have not been deposited and the client sends PScl,TN,t10, in the refraction request to any SIG TCL ~(TN)||t10 encountered gateway.

2. Refraction of deposited tickets: the client simply sends PSCL, IDDGW, t11, SIG, in the refraction request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

## 6. Accessing the Network from Foreign Domains

The accessing services visiting trust domain provided the ticketbased security infrastructure can take place in two ways including the following:

- A foreign network router MR forwards the client's new ticket request to the home domain when there is unavailable ticket for accessing the network from the foreign domain.
- An access point sends the client's ticket deposit request to the home domain when the client owns available new tickets issued by the home TA.

MR will send the network access request consisting of the symmetric key between the client and his home TA, or PSCL ticket to a gateway or network router in the client's home domain k QT outputs "accept" in Steps 1 and 2. The symmetric key between the client and MR is a $P_0$, where a,$b_p$ and $P_0$ are the public parameter of the root PKG.

## 7. Inter-Domain Authentication from Mesh Router

Inter-domain authentication is more important for wireless peer-to-peer authentication networks in this module give the inter-domain authentication. The mesh router generate theand initialize the Defense ID for each client. The client very first process generates the Resistance ID and gives the resistance ID to mesh router. The mesh router receives that ID and registers the client resistance ID and send to home domain mesh routers. The mesh router sends the defense ID to client.

## CONCLUSION

This paper identifies the problem of traffic privacy preservation in wireless mesh networks (WMN). To attack this problem, we start by introducing a lightweight architecture for WMN, then propose "traffic entropy", an information theoretic metric to quantify how well a solution performs at preserving the traffic pattern confidentiality, all of which pave the way to our penalty-based shortest path routing algorithm. Simulation results show that our algorithm is able to maximally preserve the traffic privacy, meanwhile managing the network performance degradation within the acceptable region. For the future work, we will focus on the following problems. First, multiple observing nodes may collude to analyze the traffic pattern of a destination node. Besides new routing solutions to defend collusion, we also need to extend the "traffic entropy" concept by applying the chain rules in information theory. Second, although our algorithm is evaluated in a single-radio, single-channel setting, it can be easily enhanced to exploit the advantage of multiple radios and multiple channels available in WMNs. Performance evaluation of the enhanced algorithm in such settings will be an interesting future work.

## REFERENCES

[1] S. Brands, "Untraceable off-line cash in wallets with observers," inProc. CRYPTO'93, 13th Annual Int'l Cryptology Conf. on Advances inCryptology, pp. 302–318, Aug. 1993.

[2] K. Wei, Y. R. Chen, A. J. Smith, and B. Vo, "Whopay: A scalable andanonymous payment system for peer-to-peer environments," Proc. IEEEIntl. Conf. on Distributed Computing Systems, ICDCS, July 2006.

[3] A. Menezes, P. V. Oorschot, and S. Vanston, Handbook of AppliedCryptography, Boca Raton, CRC Press, 1996.

[4] European Telecommunications Standards Institute (ETSI), "GSM 2.09:Security Aspects.," June 1993.

[5] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior inwireless networks," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp.502–516, Sept. 2005.

[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensornetworks," Comm. of the ACM, vol. 47, no. 6, pp. 53–57, 2004.

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.5, Pages : 451- 455 (2014)
*Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh*

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanismsfor large-scale distributed sensor networks," ACM Trans. SensorNetworks, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[8] W. Lou and Y. Fang, A Survey on Wireless Security in Mobile Ad HocNetworks: Challenges and Possible Solutions, edited by X. Chen, X.Huang and D.-Z. Du, Kluwer Academic Publishers/Springer, 2004.

[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE NetworkMagazine, vol. 13, no. 6, pp. 24–30, Dec. 1999.

[10] M. Raya and J-P.Hubaux, "Securing vehicular ad hoc networks,"Journal of Computer Security, Special Issue on Security of Ad Hoc andSensor Networks, vol. 15, no. 1, pp. 39–68, 2007.

[11] N. B. Salem and J-P.Hubaux, "Securing wireless mesh networks," IEEEWireless Communications, vol. 13, no. 2, Apr. 2006.

[12] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecturefor multi-hop wireless mesh networks," IEEE J. Select. Areas Communications,vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[13] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: asurvey," Comput. Netw., vol. 47, no. 4, pp. 445–487, Mar. 2005.