International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

TCAAT: Ticket Based Security Architecture Strengthened with Cellular Automata for Achieving Anonymity and Traceability in Wireless Mess Network

P. Kiran Sree[1], I. Lakshmi Pradeepa [2]

[1] *Professor,* [2] *PG student of CSE*

[1,2] *Dept of Computer Science and Engineering*

[1,2] *BVC Engineering College, Odalarevu, Allavaram mandal-533210,E.g.dt, A.P.*

Abstract: In this architecture, the conflicts between anonymity and traceability are resolved. Anonymity has received increased attention due to the users awareness of their privacy nowadays. Anonymity can be implemented to make it impossible or very difficult to find out the real author of a message. In the existing architecture Domain administrator can issues the Batch of tickets to the mobile client, it increases the mobile client's storage overhead and adversary attacks. to avoid this I present a new system in which the Domain administrator provide single Ticket to the client during the ticket issuance protocol based on the user profile which is included in agreement and It includes the renewal field for deposited Ticket. It increases the client connectivity with its home Domain administrator with considerable anonymity and traceability property and this model increases the efficiency.

***Index Terms*- Anonymity, Misbehavior, Psedonymn, revocation, Traceability, Wireless mesh network (WMN).**

I.Introduction

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs), has emerged recently. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

Conventional nodes (e.g., desktops, laptops, PDAs, PocketPCs, phones, etc.) Equipped with wireless network interface cards (NICs) can connect directly to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help the users to be always-on-line anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular, wireless sensor,worldwide inter-operability for microwave access (WiMAX) WiMedia networks. Consequently, through an integrated WMN, the users of existing network can be provided with otherwise impossible services of these networks

A wireless mesh network (WMN) [2] is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The WMN is shown in Figure 1.The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways. A mesh network is reliable and offers redundancy. **Manuscript Details Received**

When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. A Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type.wireless mesh network can be seen as a special type of wireless ad-hoc network.

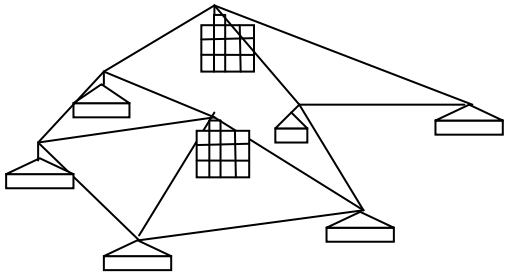

Figure 1 Wireless Mesh Network

Anonymity and traceability are left unattended. In WMNs the mobile node with high mobility can easily compromised by the adversary node in that network .so security is more important before the deployment of such networks. Nowadays user privacy is very important while accessing the network. For instance Anonymity is highly required for the honest user to unlink a user's identity to his or her specific activities in the network. And traceability is required for the misbehaved node in the network .conditional anonymity is required for the misbehaved mobile node to trace its activity by Domain Administrator (or TA). Several solutions have been proposed in WMNs to address the privacy issues for mobile users.

II.Related Works

Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Majority of security issues have not been addressed and surveyed in I.F. Akyildiz, X. Wang, and W. Wang [2].Universal pass model [3] proposed for WMNs, addressing countermeasures to wide range of attacks in WMNs. In J. Sun, Chi Zhang, Yanchao Zhang and Yuguang Fang [1]the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members generally for a long term so that Ticket –based security architecture was developed which includes Ticket issuance, Ticket deposit, .Design of a ticket-based anonymity system with traceability property; bind of the ticket and pseudonym which guarantees anonymous access control (i.e., anonymously authenticating a user at the access point and simplified revocation process ,revocation of Tickets, adoption of the hierarchical identity-based cryptography (HIBC) for interdomain authentication avoiding domain parameter certification are illustrated in[1].the following figure[fig 1] explains the Ticket issuance and Deposit phase[1].

Ticket Issuance

Here Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to reveal his real ID to the TA(Trusted Authority) in order to obtain a ticket since the TA has to ensure the authenticity of this client. After some process TA issues batch of Tickets to MN (mobile Node) . The ticket generation algorithm[1], which can be any restrictive partially blind signature scheme in the literature, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket . A design issue to be pointed out is the commonly agreed information c negotiated at the beginning of the ticket generation algorithm. We define C as (ticket value, expiry date, misbehavior,) , where Ticket Value- the total amount of traffic that the client is allowed to generate and receive before the expiry date of the ticket Misbehavior-Ticket reuse and multiple deposits Expiry date-Ticket expiry date (validity period) After obtaining a valid ticket, the client may deposit it Anytime the network service is desired before the ticket expires, using the ticket deposit protocol . The DGW then creates a record for the deposited ticket as: record =(ticket,-,-, rem, log),where log field is created to record such noncompliant behavior [1].misbehavior is totally different from noncompliant behavior.

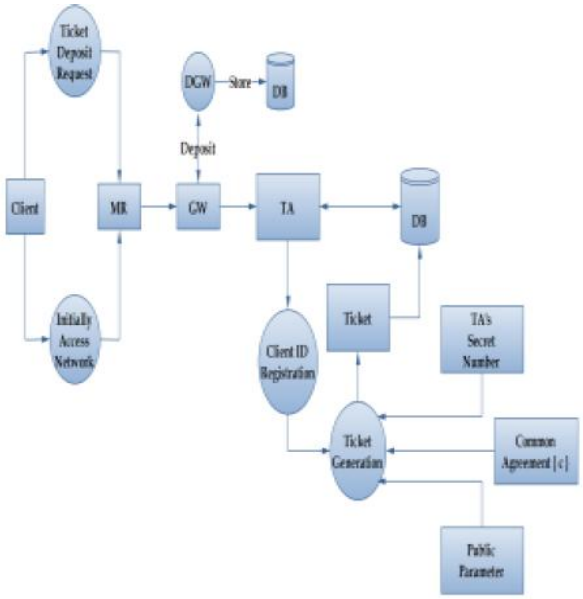

Fig 1.Ticket issuance and deposit

IV Existing System

In wireless communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet forwarding path than in wired networks. Thus, routing anonymity is indispensable, which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly

desirable such as in e-cash systems where it is used for detecting and tracing double-spenders.

Each client can get the batch of Tickets during the Ticket issuance phase, so that client memory will be increased. And it place extra overhead in revocation process of unused Tickets. Here Ticket value is assigned based on past misbehavior history of mobile node (client), there is no possible decision making function during the Ticket generation process for the mobile node who want to be a permanent user within that trust domain.

IV Proposed System

Blind Signature

In general, a blind signature scheme allows a receiver to obtain a signature on a message such that 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, unlinkability, 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. As the name suggests, this property restricts the user in the blind signature scheme to embed some account-related secret information into what is being signed by the bank (otherwise, the signing will be unsuccessful) such that this secret can be recovered by the bank to identify a user if and only if he double-spends. The restrictiveness property is essentially the guarantee for traceability in the restrictive blind signature systems. Partial blind signature the resulting signature to convey publicly visible information on common agreements between the signer and the signee. This is useful when certain information in the signature needs to be reviewed by a third party. One example is the common agreements, the visibility of which enables the intermediate parties who examine the signature to check the compliance of the signee to the items specified in the agreements, before proceeding to the verification of the signature and other operations. Restrictive partially blind signature schemes were derived from the aforementioned work. They are essentially 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.

Restrictiveness.

Let a message m be such that the receiver knows a representation $(a_1; \ldots; a_k)$ of m with respect to a generator tuple $(g_1; \ldots; g_k)$ at the beginning of a blind signature protocol. Let $(b_1; \ldots; b_k)$ be the representation the receiver knows of the blinded message m_0 of m after the completion of the protocol. If there exist two functions i_1 and i_2 such that $i_1(a_1; \ldots; a_k) = i_2(b_1; \ldots; b_k)$, regardless of and the blinding transformations applied by the receiver, then the protocol is called a restrictive blind signature protocol. The functions I_1 and I_2 are called blinding-invariant functions of the protocol with respect to $(g_1; \ldots; g_k)$.

Partial Blindness.

A signature scheme is partially blind if, for all probabilistic polynomial-time algorithm A, A wins the game in the signature issuing protocol with probability at most ½ + 1/ k for sufficiently large k and some constant □. The probability is taken over coin flips of KG, U0, U1, and A, where KG is the key generation function defined in U0 and U1 are two honest users following the signature issuing protocol. Due to the space limitation, interested for complete description of the game in the signature issuing protocol.

Ticket Generation based on user profile

In order to maintain security of the network against attacks and the fairness among clients, the home TA may control the access of each client by issuing tickets based on the misbehaviour history of the client, which reflects the TA's confidence about the client to act properly. Ticket issuance occurs when the client initially attempts to access the network [1][fig 2]

Fig 2.WMNs with Trusted Authority

The proposed system includes the common agreement c(Val, exp , Mis , User Profile) for obtaining ticket from Domain Administrator(i.e. TA).

User Profile consists of 1) Long Term User with less anonymity 2) Short Term User with high anonymity based on this the client can get the suitable ticket value (Min or Max).restrictive Partially blind signature scheme is used for achieving anonymity for user [1] which borrows the blind signature technique [5][6][7] to achieve anonymity.ID based cryptography used for authentication purpose.

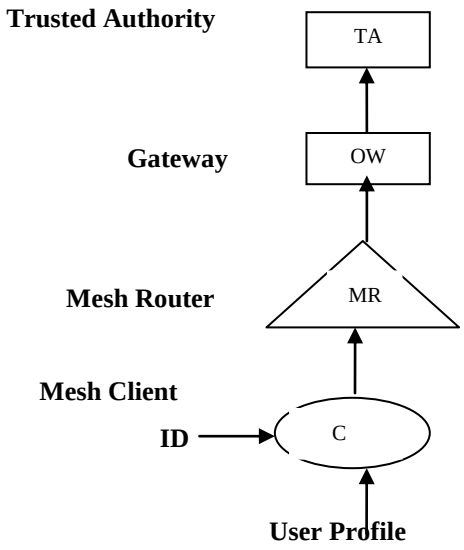

Figure 3: profile based ticket request

The mobile client can enter its ID and related information along with User profile to TA to get the Ticket [Fig 3].

Long Term User with less anonymity

If the client initially entered into the network, he or she can request Ticket from the TA to access the internet with free of cost .first the TA authenticates the client then it issues the Ticket to achieve anonymity and traceability of client. If the clients want to be a permanent user in particular domain, he or she uses this field. During the ticket generation protocol if the client sends this common agreement (c)
C (Val, exp, Mis, Long Term User)
Then the TA does the following steps
checks the past misbehavior history of the corresponding client
If (mis=0) then
checks the client anonymity requirement
Status
If (anonymity=not strict)

Short Term User

The common agreement(c) , C(Val, exp, Mis, short Term user) is used to get the Ticket with lower value. Normally TA sets the lower value for the misbehaved clients to punish the clients. In addition if the mobile client having high mobility and it needs strict anonymity scheme, this field is used. The TA checks the user profile field in the C and assigns the value based on user requirements.
Note: The user profile can be varied for each time based on anonymity requirement of corresponding user.

Deposited Ticket Renewal Process

After depositing a Ticket on a GW, the client can access the services until the Ticket expired, in the following cases the client can request Renewal process. The record generated by GW to the deposited ticked and forwarded to TA. This includes Renewal request.

Case 1: deposited ticket value is depleted before the expiry time.
Renewal request processing steps
1 .DGW informs the Client
(i.e. c(val=0,mis=0,exp=not expired))
2 If the Client wants renewal then
Renewal (ticket)
Else
Revocation (ticket)
3. DGW sends the request to TA

4. DGW and TA databases are updated

Case 2: The client wants to access the internet under the same ticket. i.e. the following condition
C (Val=0,mis=0,exp=expired)

Renewal process applicable only for the deposited Ticket (mis=0), and renewal process doesn't give fresh Ticket, it will increase the Ticket value for few seconds only .computation complexity increased for GWs in which renewal process is carried out.

Security Analysis

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system

cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack.

Fundamental security objectives

It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption, in our system. We are only left with the proof of non repudiation in this category. A fraud can be repudiated only if the client can provide a different representation ðu1; u2Þ he knows of m from what is derived by the TA. If the client has misbehaved, the representation he knows will be the same as the one derived by the TA which ensures non repudiation.

Traceability (conditional anonymity)

According to its definition, this requirement is twofold: 1) Anonymity for honest clients is unconditional,
2) A misbehaving client is traceable where the identity can be revealed. The proof of point 2 follows from [32, Theorem 2] that the adopted restrictive partially blind signature scheme in our security architecture achieves restrictiveness. In other words, point 2 states that the client can only obtain signatures on messages of which the client knows a representation for which the structure in the representation (where the identity information is encoded) remains and two extra requirements on the representations the client knows of m and m0 .

Framing resistance

If the client is honest, with overwhelming probability, the representation (u1, u2) he knows is different from that the malicious TA falsely generated. Since the client could not have come up with this representation by himself, it proves that the TA attempts to frame the client. Therefore, innocent clients can exculpate themselves to prevent malicious TAs from revoking their network access privilege.

Unforgeability.

The proof of unforgeability that the adopted restrictive partially blind signature scheme is existentially unforgeable against adaptively chosen message and ID attacks under the assumption of the intractability of CDHP in G1 and the random oracle.

We conclude that the proposed security architecture satisfies the security requirements for anonymity, traceability, framing resistance, and un forge ability, in addition to the fundamental objectives including authentication, data integrity, confidentiality, and non repudiation, under the assumption that CDHP in G1 is hard and the random oracle.

Efficiency Analysis

In existing a batch of Tickets is assigned to requested clients, but in this proposed model restriction applied for client requested message i.e. a client can get single Ticket during the ticket generation process. It decreases the client's storage overhead. The renewal process decreases the computation overhead of client. Revocation processes of unused tickets are eliminated. If the client wants another Ticket, it must initiate the revocation process for the old.

The inter domain access is enabled by the hierarchical ID-based cryptosystem, the implementation of which largely determines the efficiency of the inter domain access. The communication and computation efficiency is best achieved using the Dual-HIDS
The client transmits approximately 148 bytes and 446 bytes respectively, for a new ticket request and a ticket deposit request. They correspond to the transmission time of 1.18 and 3.57 ms, respectively, assuming a 1 Mbps communication link between the client and the gateway. In the new ticket request, the client needs to perform an HIDS signing and verification, a symmetric-key encryption, and an HMAC, among which the HIDS operations dominate the computation costs. The signing involves only four point multiplications (three for HIDS and one for deriving the symmetric key), one point addition, and one hash evaluation, and can be efficiently carried out160bit HMAC output), respectively, for a new ticket request and a ticket deposit request.

Communication

Our ticket-based security architecture consists of four intradomain protocols in which ticket deposit involves only clients and gateways. This protocol is distributed in nature, and thus, the communication cost incurred is more

affordable. In contrast, protocols involving interactions with the centralized TA contribute largely to the expensive communication costs in the system. In the fraud detection protocol, gateways report accumulated ticket records to the TA periodically instead of in real time. Reports from gateways can be scheduled at different time intervals, avoiding a sudden increase in the communication overhead caused by simultaneous transmissions.

Ticket issuance and revocation may take place in real time. The associated communication overhead depends on how frequent 1) the clients use up issued tickets and 2) the clients misbehave. One can expect minimal real-time interaction with the TA for systems where ticket issuance is based on the client's usage trend (such that ticket requests other than scheduled will be infrequent) and there is a wellbehaving majority. Since multiple tickets are issued to the client at each scheduled interval, the average communication cost can be further reduced because some parameters need only be transmitted once. In a single ticket issuance, the client sends roughly 60 bytes (i.e., three 160-bit elements) to the TA. The TA sends to the client approximately 128 bytes (i.e., four G1 elements and two 160-bit HMACs).

Storage

The TA may consist of several servers to store necessary information from all clients during protocol executions. The storage capability of these high end servers is usually not a concern, and therefore, we focus on the storage overhead encountered at the low-end client side.

Fortunately, many pairing operations in the protocols can be computed once and stored for future use. Furthermore, some stored information remains unchanged for all instances of protocol execution (e.g., all tickets issued in the ticket issuance protocol). As a result, we need merely take into account the effective storage overhead (i.e., information that is changed and has to be stored at each protocol instance).

In ticket issuance, the client stores for each protocol Instance 621 bytes pre computed information and 43 bytes after-protocol information for future use.

Computation

In ticket issuance, the client only computes two basic pairings in real time for each protocol instance. The remaining pairing operations can either be computed once or be pre computed and stored for all protocol instances. Several HMAC operations also need to be performed in real time, which is considered computationally efficient. In ticket deposit, one signing, one verification, and two HMAC operations are performed in real time by the client for each ticket deposited. All pairings involved in this protocol can be pre computed except one for the verification. A finite field exponentiation is needed for the signing. Similarly, in ticket revocation, a client has to compute one signature in real time for each revoked

V. Conclusion

In this paper, we propose a security architecture mainly consisting of the User ticket-based protocols, in which Ticket was generated based on user profile (anonymity requirement) which resolves the conflicting security requirements of unconditional anonymity for honest users and traceability of misbehaving users and the single Ticket is issued to every client so that storage overhead was reduced and it enhanced with Ticket renewal process. By utilizing the tickets based on user profile, the proposed architecture is demonstrated to achieve desired security objectives and efficiency. Ticket, which requires no basic pairings but a finite field exponentiation.

REFERENCES

[1] IEEE transactions on Depentable and Secure computing vol 8, NO.2 march-april 2011 SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang,

[2] I.F. Akyildiz, X. Wang, and W. Wang, Wireless Mesh Networks: A Survey,‖ Computer Networks, vol. 47, no. 4, pp. 445-487, Mar. 2005.

[3] Y. Zhang and Y. Fang, ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks, IEEE J. Selected Areas Comm., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[4] .X. Chen, F. Zhang, and S. Liu, ID-Based Restrictive Partially Blind Signatures and Applications, J. Systems and Software, vol. 80, no. 2, pp. 164-171, Feb. 2007.

[5] S. Brands, Untraceable Off-Line Cash in Wallets with Observers,Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cyptology (CRYPTO '93), pp. 302-318, Aug. 1993.

[6] K. Wei, Y.R. Chen, A.J. Smith, and B. Vo, ―Whopay: A Scalableand Anonymous Payment System for Peer-to-Peer Environments,‖ Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), July 2006.

[7] D. Chaum, ―Blind Signatures for Untraceable Payments, Advancesin Cryptology—Crypto '82, pp. 199-203, Springer-Verlag, 1982.

[8] J. Sun, C. Zhang, and Y. Fang, ―A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks, Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008

P.KIRAN SREE received his B.Tech in Computer Science & Engineering, from J.N.T.U and M.E in Computer Science &Engineering from Anna University.
He is pursuing Ph.D in Computer Science from J.N.T.U, Hyderabad. His areas of interests include Cellular Automata, Parallel Algorithms, Artificial Intelligence, and Compiler Design. He was the reviewer for many International Journals and IEEE Society Conferences on Artificial Intelligence & Image Processing. He also nominee for Marquis Who's Who in the World, 28th Edition (2011), USA.

I Lakahmi Pradeepa, received the B.Tech degree in Computer Science &Engineering from J N T University. She is pursuing M.Tech in Computer Science &Engineering from J.N.T.U, Kakinada.