A MULTI LAYER AUTHENTICATION APPROACH FOR ROUTING IN MESH NETWORKS

P.Ramya[1], A.Komathi[2]

[1]Research Scholar, [2]Department of CS & IT,

Nadar Saraswathi College of Arts and Science, Theni, (India)

ABSTRACT

The Issues of risk-free multicast of data streams across a multihop wireless ad hoc network has been dealt with respect to this analysis. So as to fix the particular issues of ad hoc networks a dynamic multicast group management protocol has been endorsed. The prime concept behind it is, the group users dynamically take part in the stability of multicast group thereby decreasing the communication and computation strain on provider. To assess that a node is permitted to connect the group, as well as a related abrogation system. A Hierarchical Anonymous Authentication Topology (HAAT) has been endorsed is a novel stable communication model, that has been designed for WSNs.In one part HAAT applys harsh Source sensor access control to deal with the either liberate competitors in addition to spiteful Source sensors. On the other part, it provides challenging Source sensor confidential stability close to either antagonist with a range of different network bodies. HAAT is a collection of affirmation and prime agreement protocol developed based on our HAAT.As per the research the HAAT is convenient to numerous stability and confidentiality related problems.

Keywords: Anonymous, Hierarchical Anonymous Authentication Topology, Network Operator, Relay, Source Sensor

I. INTRODUCTION

For steady dispersion as well as spreading of data through wireless multihop ad hoc networks (MANET) is one significant study challenge is the way to control the data accessibility to the bunch of permitted nodes. Encoded data should be decoded simply through permitted members. The group stability should be managed while ne users enroll/exit as well as a node is terminated. The challenge described as below: provided single source multicasting a data stream with numerous receivers that connect/exit the multicast program, the aim is to develop a minimal protocol which enables permitted nodes and just permitted nodes to retrieve the data stream multicast through the source node. Hence the steady multicast group management protocol must consider erratic links, nodes portability and restricted communication and calculation ability of the nodes.

Mohamed Younis et al endorsed novel Tiered Authentication technique for Multicast traffic (TAM) great measure heavy ad-hoc networks nodes are assorted in to clusters. Multicast traffic found in the same cluster implements single means of range so as to validate the communication provider. Cross-cluster multicast traffic comprises a message authentication codes (MACs) which are stand on a collection of keys or ideas. Every cluster makes use of unique subset of keys to check it’s concerning unique grouping of authentic MACs in the message classify to validate the provider. Therefore TAM integrates hidden data irregularity and time uncertainty or abnormality standards also makes use of network clustering to minimize expense and assure scalability. Mohamed Younis et al endorsed design provided inspiration, it has been suggested here a novel layered protocol makes use of vicinity to minimize the communication difficulty of steady multicast for active groups of mobile multihop nodes. It has been intended to minimize the entire network communication expenses employing any form of group link or join.

The support has been quadruplicated as below:

Security: accomplishes specific common verification and an essential group between Source sensors and relay sensors also between Source sensors independently. Hence it limits either illicit network usage from liberate competitors and spiteful Source sensors and spiteful assaults as a result of sneaky relay sensors.

Anonymity: Simultaneously allows freelance unknown verification between Source sensors and relay sensors also two-sided unknown verification among any two Source sensors. Hence ensure Source sensor privacy and confidentiality.

Accountability: Allows Source sensor responsibility to control Source sensor characteristics thereby WSNs from getting impaired and assaulted. Network communications continually checked regarding arguments and illusions, and also permits transformative Source sensor abrogation to ensure spiteful Source sensors might be evicted.

Sophisticated Source sensor privacy: Permits Source Sensors to expose smallest data possibility when maintains or conserves responsibility. Source sensor behaviors in HAAT, is a complete data like network Source sensors since group users regularly communicate with WSNs in various functions and perspectives. Instead of revealing complete individual data, a disagreement about a provided communication program must exclusively link based on the functions/perspective data regarding the Source Sensor.

HAAT is the very first effort to arrange a responsible security structure with a complex confidential security system customized for WSNs.Additionally HAAT sets a sound foundation for developing other top level security and confidentiality that is unknown communication.

II. RELATED WORK

Past study in the field of steady and secure multicast has primarily centered on wired networks along with several methods had been endorsed looking at numerous limitations in [16-29]. The primary constraints of such algorithms that they had not been developed for multihop wireless ad hoc networks. The design of a rational key tree is a most popular method in which group users are connected with leaves thereby providing all the users all the keys. The root key is the group key concept enables minimizing the communication expense for key revision, in case of group account modification, to O(log M) in which M is the range of group users. Numerous plug-ins had been endorsed to address the stability or security in [14], node dependent group dynamic in [31], and time variant group dynamic in [19, 26]. Plug-ins to wireless networks had been initially described in [32] and numerous secure multicast protocols had been endorsed in [33-35].Above protocols deals with either challenges associated to portability and instability. Anyways the protocols are primarily centered on single hop wireless networks in which base stations or satellite beams deal with significant locations. Substantial energy preserving could be attained for secure multicast across ad hoc networks through inserting the nodes on the key tree as per the actual area. The endorsed heuristics deals with the situation of active groups in which the nodes are non-portable or with quite less portability.

Mohamed Younis et al presented a novel Tiered Authentication strategy for Multicast traffic (TAM) for high degree heavy ad-hoc networks. Nodes are arranged into clusters. Multicast traffic in the equivalent cluster applies one-way range is classifies to validate the information resource. Cross-cluster multicast traffic contains a message authentication codes (MACs) which banks on a groups of keys. Every cluster employs a distinct subset of keys to check for its different collection of logical MACs in the message so as to authenticate the source.The field of securing ad hoc and sensor network attained significant attention in the past couple of years and numerous methods and protocols had been endorsed key pre-dispersion to permit secured connectivity, security towards assertion of work in [36-38], implementing equity in [39], verification and stability of data streams. Such numerous methods are balancing our task in protecting the ad hoc network.

By disabling ends of communication link Onion Routing attains privacy in [11]. An Onion routing network is made up of a range of integrated Onion routers (ORs) where every OR has a number of public/private keys. Every OR understands the topology of the Onion network plus the public keys of the other ORs.The destination source sensor referred as the Onion Proxy (OP) for the Source sensor which demands an private communication might appeal to an OR on which it relies.The destination Source sensor and its OP is secured from its rivalries through the communication between the both. The OP wraps up a route or path which is made up of group of ORs and build an "Onion" employing the public keys of the routers on the way. The "Onion" is built in such a manner that most of the interior portion is the message to the desired location. The information is covered or encoded in a systematic way like the Ors looks in the route. The moment an OR acquires the Onioned information it employs its private key to remove that is decoding the "Onion", to get in a systematic way like subsequent hop and the session key. Then it delivers the remaining "Onion" to the later hops. This process is reiterated till the "Onion" achieves final OR, that removes preceding level or layer of the "Onion" and get the passage in an order , is the final location.

In an Onion route simply the proxy is aware of the initial and end or destination router .Whatever OR in the route simply aware of its preceding hop and subsequent hop. For both external and internal assaulters as encryption or decryption (encoding or decoding) is development at each OR.Its tough to connect any two links to the same route. Hence a communication moving through the Onion routers, the entering OR and the outlet OR are unable to connect.Whenever will find a numerous links, it is difficult to enter and exit the two communication ends concerning connections which employs onion routing.

To skip the modification "Onion"in the route settled stage perhaps offer adversary clues regarding routing in plan, an "Onion" should be cushioned while section of it is in series has been studied and eliminated,to ensure the extent of the "Onion' for an internal viewer to get the routing in order.It has been recommended ,if most of Onion routers in aprivate route is N,the Or will build message of N "Onions" to establish an Onion route.A router decodes all "Onion"s,while a router gets the "Onions “and obtain the routing information simply from the initial one in [10].

2.1 Group Signature

Chaum and van Heyst in 1991 presented a Group signature strategy, is a relatively latest cryptographic concept in [9]. A group signature strategy is a method for permitting group users to subscribe a communication with respect to the group. In contrast to normal signatures, that provides privacy to the subscriber that is an examiner can just determine that the users of any group has signed. A legal squabble is an exceptional situation, where any group signature is usually "opened" through specified group management to generate plainly known the characteristics of the signature's creator.Certain group signature strategies maintain annulment in which group users might be incapable. Boneh and Shacham forecasted a most latest group signature strategy in [8] has a completely brief signature length in [10].This strategy is relies on the next two issues that are assumed to be difficult. Let G_1, G_2, g_1, g_2 as described on top.

III. PROBLEM FORMULATION AND THE SCHEME OVERVIEW

3.1 Network Architecture and System Assumptions

The three-layer structure under the administrator of a network operator (NO) points to a metropolitan-scale WSN. The network operators utilizes numerous APs and relay sensors thereby developing a perfectly linked WSN which handles the complete region to network Source sensors that is the residents. Further the Network Source sensors sign up to the network operator for the solutions and apply their mobile customers to easy access of the network from anywhere inside the city. The subscription of network Source sensors will probably 1. Finished/revived as per Source sensor- operator contract in a disrupted fashion or 2) In the matter of debate/assault, actively terminated by NO.

It has been assumed that downlink from a relay sensor to all Source sensors inside its area is one hop same as in [4], [11].Conversely, the uplink from a Source sensor to a transmit sensor might be single or multiple hops. A network Source sensor need to send packets in various hops to a relay sensor outside its direct transmission range. Network Source sensors help one another on passing on the packets to relay sensors. It has been supposed that all the network traffic need to move over a relay sensor apart from the communication between the two direct adjacent Source sensors. It has been anticipated that the communications back and forth of a relay sensor will develop most of the traffic in a WSN in [12] thereby minimizing the routing difficulty from the Source sensor's angle involves the duty.

It is supposed that communication through relay sensors previously known protected networks, and hence relates them. The WSN is supposed to be implemented repeatedly in thought which allows annulment of unique relay sensors are not going to impact network link. It has been thought of an offline trusted third party (TTP) that reliable for concealing the information it holds. TTP is important during the process implementation and can find a protected channel between TTP and every network Source sensor.

3.2 Threat Model and Security Requirements

WSNs are vulnerable to both static and dynamic assaults ,as a result of the open medium and spatially displayed nature The unaggressive assaults incorporates eavesdropping when active simulation to relay sensor collaboration. It has been taken into account an antagonist for a functional risk system is capable of eavesdrop all network communications plus add arbitrary bogus messages. Also the antagonist can settle and manage the less number of Source sensors and relay sensors referred to its alternative. Also establish rogue relay sensors to phish Source sensor usage. The performance of the antagonist incorporate 1) prohibited and irresponsible network usage, 2) the confidentiality authentic network Source sensors, and 3) denial-of-service (DoS) assaults in opposition to service availability.

There are some crucial privacy specifications in order to ensure that a WSN performs correctly properly and firmly as intended are presented below:

• Source and relay sensor shared authentication and key agreement: To prevent mutual illegal network access and Phishing assaults, both relay and source sensor uniformly authenticate one another and also establish a common pair wise symmetric key for validating the session and encoding the message.

• Hop Level Sensors mutual authentication and key agreement: Source sensors through cooperation, authenticating one another to monitor message relaying and routing. Symmetric keys provides session authentication and encoding of message are standard one and should be managed effectively across the similar traffic.

IV. HAAT: HIERARCHICAL ANONYMOUSAUTHENTICATION TOPOLOGY

It has been noticed during developing HAAT that, unlikely available private responsible cryptographic primitives like blind mark and group signature strategy, meets the thought provided reliability and security demands. Blind signature and group signature strategies could merely provide joining secretly, whereas HAAT requires Source sensor accountability, thus revocable privacy. Prevailing group signature strategies provide revocable privacy, however unable to maintain complex Source sensor security. It enables a group signature strategy has been customized through merging with onion ring scheme to convoke every requirements. HAAT developed on the onion ring oriented group signature divergence through additionally combining this into the validation and key contract protocol model.

4.1 HAAT Key Management

Below arranged processes are implemented in an offline means through all the possibilities in HAAT, especially NO, a TTP, relay sensors, network Source sensors, and Source sensor group managers. HAAT performs under bilinear groups with isomorphism and specific originators also as in Section 2.1. HAAT also utilizes hash functions and H_0 and H, with respective ranges G_2^2 and Z_p .The information beneath primarily employs in [8].

NO is liable for the key generation operation. Especially NO continues as below

1. Select a generator g_2 in G_2 uniformly at arbitrary and set $g_1 \leftarrow \psi(g_2)$. Select $\gamma \underset{\leftarrow}{R} Z_p^*$ and set $w = g_2^{\gamma}$.
2. **Select** $grp_i \underset{\leftarrow}{R} Z_p^*$ For a subscribed source sensor group I**,**
3. Using γ , generate an SDH tuple $(A_{i,j}, grp_i, x_j)$ by selecting $x_j \underset{\leftarrow}{R} Z_p^*$ such that $\gamma + grp_i + x_j \neq 0$, and setting $A_{ij} \leftarrow g_1^{1/(\gamma + grp_i + x_j)}$.
4. Repeat Step 3 for a pre-organized number of times that are collectively conesented by *NO* and the Source sensor group manager GM_i .
5. Send $GM_i\{[i, j], grp_i, x_j) | \forall j\}$
6. For every Source sensor group.
7. Send *TTP:* $GM_i\{[i, j], A_{i,j} \otimes x_j) | \forall i, j\}$ through channel,.

Additionally, *NO* prepares every relay sensor MR_k a public/private key pair, denoted by (RPK_k, RSK_k) . Each relay sensor also gets an accompanied public key

$Cert_k = \{MR_k, RPK_k, ExpT, Sig_{NSK}\}$, Before accessing the WSN, a network Source sensor has to check Source sensor groups. For each such Source sensor group i, a network Source sensor uid_j provide group private key :

1. GM_i sends $uid_j(|i, j|, grp_i, x_j)$ as well as the related system parameters.
2. GM_i requests *TTP* to send $uid_j(|i, j|, A_{i,j} \otimes x_j)$ by providing the index [i, *j*].
3. uid_j assembles his group private key as $gsk[i, j] = (A_{i,j}, grp_i, x_j)$.

Note that in our setting,

- GM_i only keeps the mapping of $(uid_j(|i, j|, grp_i, x_j))$ but has no knowledge of the corresponding $A_{i,j}$.
- *TTP* has to mapping of $(uid_j(A_{i,j} \otimes x_j, grp_i))$ as it sends uid_j this information. But *TTP* has no knowledge of the corresponding x_j or $A_{i,j}$.

Here, uid_j signs on the messages it receives from GM_i and *TTP* under ECDSA-160, and sends back GM_i the equivalent signature.

4.2 Source and Relay Sensor Mutual Authentication and Key Agreement

To access the WSN, a network Source sensor follows the source and relay sensor when a relay sensor is within his direct communication range.

1. The relay sensor MR_k first picks a random nonce $r_R \underleftarrow{R} Z_p^*$ and a random generator g in G_1 and then computes $g^{r_R}.MR_k$ further signs on $g\,g^{r_R}$, and the current time stamp ts_1, using ECDSA-160. *MR$_k$* then broadcasts

$g, g^{r_R} ts_1, Sig_{RSK_k}, Cert_k, CRL, URL$ (M.1)

Here, *CRL* and *PACKET* denote the relay sensor certificate revocation list and the Source sensor revocation list, respectively.

Compute $T_1 \leftarrow u^{\alpha} and T_2 \leftarrow A_{i,j} v^{\alpha}$ by selecting an exponent $\alpha \underleftarrow{R} Z_p . Set \delta \leftarrow (grp_i + x_j)\alpha \in Z_p$. Pick blinding values r_α, r_x, and $r_\delta \underleftarrow{R} Z_p$.

Compute helper values R_1, R_2, and R_3 :

$R_1 \leftarrow u^{r_\alpha}, R_2 \leftarrow e(T_2, g_2)^{r_x}.e(v, w)^{-r_\alpha}.e(v, g_2)^{-r_\delta}$, and $R_3 \leftarrow T_1^{r_x}.u^{-r_\alpha}$. Compute a challenge value $c \in Z_p$ using ***H:***

$c \leftarrow H(gpk, g^{r_j}, g^{r_R}, ts_2, r, T_1, T_2, R_1, R_2, R_3) \in Z_p.$

Compute $s_\alpha = r_\alpha + c\alpha, s_x = r_x + c(grp_i + x_j)$ and $s_\delta = r_\delta + c\delta \in Z_p$. Obtain the group signature on $\{g^{r_j}, g^{r_R}, ts_2\}$ as

$SIG_{gsk[i,j]} \leftarrow (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$.

Compute the shared symmetric key with MR_k ***:***

$K_{k,j} = (g^{r_R})^{r_j}$.

Unicast back to MR_k

$g^{r_j}, g^{r_R}, ts_2, SIG_{gsk[i,j]}$. ***(M.2)***

Upon receipt of (M.2), MR_k carries out the following to authenticate uid_j :

Check g^{r_R} and ts_2 make sure the freshness of (M.2).

Check that $SIG_{gsk[i,j]}$

Compute $\hat{u}$ and $\hat{v}$ using (**1**), and their images

u and ***v*** in $G_1 : u \leftarrow \psi(\hat{u}) and v \leftarrow \psi(\hat{v})$.

Retrieve R_1, R_2 and R_3 as:

$\tilde{R}_1 \leftarrow u^{s_\alpha} / T_1^c$

$\tilde{R}_2 \leftarrow e(T_2, g_2)^{s_z}.e(v, w)^{-s_\delta}.(e(T_2, w)/e(g_1, g_2))^c$,

And $\tilde{R}_3 \leftarrow T_1^{s_z}.u^{-s_\delta}$.

Check that the challenge c is correct:

$c \underset{=}{?} H(gpk, g^{r_j}, g^{r_R}, ts_2, r, T_1, T_2, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3)$. (2)

For each revocation token A $\in$ PACKET, check whether A is encoded in (T_1, T_2) by checking if

$e(T_2 / A, \hat{u}) \underset{=}{?} e(T_1, \hat{v})$. (3)

MR_k is now assured that the current Source sensor is a legitimate network Source sensor, although MR_k does not know which particular Source sensor this is. MR_k Further computes the shared symmetric key as $K_{k,j} = (g^{r_j})^{r_R}$ and sends back uid_j :

$g^{r_j}, g^{r_R}, E_{K_{k,j}}(MR_k, g^{r_j}, g^{r_R})$, (M.3)

Upon successful completion of the protocol, the relay sensor and the Source sensor is uniquely identified through (g^{r_j}, g^{r_R}).

4.3 Hop Level Sensors Mutual Authentication and Key Agreement In HAAT

Adjacent genuine network Source sensors may help to relay each other's traffic. To this end, two network Source sensors within each other's direct communiqué range first authenticate each other and produce shared secret pairwise key as follows:

1. uid_j picks a random n once $r_j \underset{\leftarrow}{R} Z_p^*$ and computes where g^{r_j} is obtained from the inspirational messages broadcasted by the current check relay sensor.
2. Upon receipt of $(\tilde{M}.1)$, uid_I c uid_I Further checks if the signature is produced from a revoked group private key following Step 3c, as in Section 4.2.
3. uid_I is assured that the in progress Source sensor it communicates with is legitimate. uid_I proceeds to

pick a random nonce $r_I \underset{\leftarrow}{R} Z_p^*$ and computes g^{r_I} . uid_I further signs on g^{r_j}, g^{r_I}, and current time stamp ts_2, using an suitable group private key gsk[t, I] of his. uid_I also computes the shared pairwise session key as $K_{r_j,r_I} = (g^{r_j})^{r_I}$. then replies uid_I

$$g^{r_j}, g^{r_I}, ts_2, SIG_{gsk[t,I]}. \qquad (\tilde{M}.2)$$

3. Upon receipt of $(\tilde{M}.2)$, uid_j first delay window. uid_j checks whether ts_2 - ts_1 is within the satisfactory delay window. uid_j also examines $SIG_{gsk[i,j]}$ and *PACKET* as uid_j did above. If all checks succeed, uid_j is also certain that its communicating counterpart is legitimate. uid_j Computes the shared pair wise session key as $K_{r_j,r_I} = (g^{r_I})^{r_j}$. uid_j Finally replies uid_I

$$g^{r_j}, g^{r_I}, E_{K_{r_j,r_I}} = (g^{r_I}, g^{r_I}, ts_1, ts_2). \qquad (\tilde{M}.3)$$

Upon receipt of $(\tilde{M}.3)$ and successful decryption of $E_{K_{r_j,r_I}} = (g^{r_I}, g^{r_I}, ts_1, ts_2)$. uid_I is assured that uid_j has effectively completed the authentication protocol and predictable the shared key for their succeeding communiqué session, which is uniquely recognized through (g^{r_j}, g^{r_I}).

V. PERFORMANCE ANALYSIS OF HAAT

5.1 Performance Analysis

Communication overhead (see figure 1): In HAAT, Both authentication and key agreement protocols need only three-way communication among relay sensors and network Source sensors and among network Source sensors. HAAT poses minimum additional communication overhead on network Source sensors to relay sensors. In messages (M. 1), $(\tilde{M}.1)$, and $(\tilde{M}.2)$, a network Source sensor only needs to broadcast a group signature to accomplish the authentication function. Group signature difference in the scheme proposed in [8], the signature comprises two elements of G_1 and five elements of G_1. When using the curves described in [19], one can take p to be a 170-bit prime and as a group G_1, where each element is 171 bits. Thus, the total group signature length is 1,192 bits or 149 bytes. With these parameters, security is about the same as a standard 1,024-bit RSA signature, which is 128 bytes [8].

Computational overhead (see figure 2)*:* In HAAT, the signature generation and verification are two important operations. By design, HAAT adopts an asymmetric-symmetric hybrid approach for session authentication to decrease computational cost. Network entities (both relay sensors and network Source sensors) execute exclusive group signature operation to authenticate each other only when establishing a new session; all subsequent data exchanging of the same session is authenticated through a highly efficient MAC-based approach.

Storage overhead: In HAAT, network Source sensors may carry resource-constrained persistent devices such as PDAs and smart phones to access the WSN. Therefore, storage overhead for each network Source sensor should be reasonable to modern pervasive devices. As is shown in our scheme description, each network Source sensor in HAAT needs to store two pieces of information: his group private key and the related system parameters. The group private key for each Source sensor just contains 1 group element of G_1 and 2 elements of Z_p^*. If we choose p to be a 170-bit prime and as a group G_1 with each group element of 171 bits, the group private key for every Source sensor just consumes 511-bit memory, which is insignificant for modern pervasive devices. The most memory-consuming parts are the system parameters, which may contain codes to describe the bilinear groups (G_1 and G_2), the bilinear pairing function (e), the isomorphism ψ, the hash functions $(H_0 and H_1)$, and the signing function ECDSA-160. Fortunately, the needed code size for each part could be in the magnitude of kilobytes as is studied in prior work such as [20]. Therefore, it should be affordable to most of the modern pervasive devices.

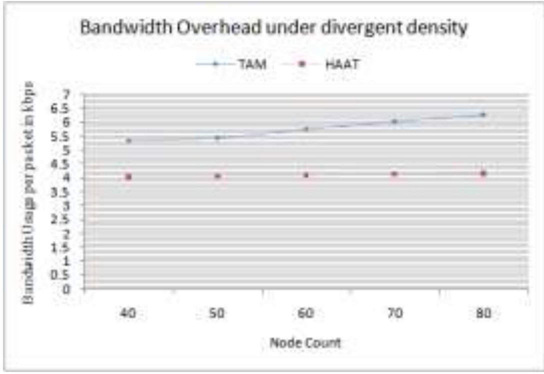

Figure 1: Communication Overhead Representation by the Usage of Bandwidth

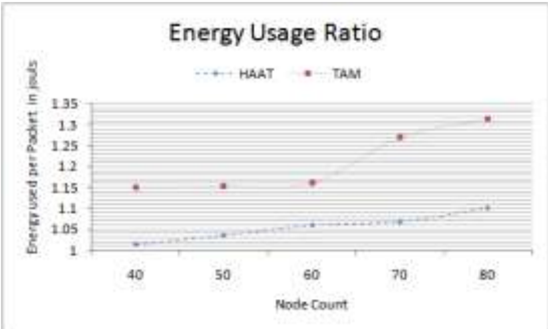

Figure 2: Computational Overhead Representation by the Usage of Energy Resources

VI. CONCLUSION

In this paper, we proposed HAAT, to set up an liable security framework with a complicated Source sensor privacy protection model tailored WSNs. The group signature scheme[8] that combined with onion ring strategy [31]. We then built HAAT on this new model by further integrating it into the authentication and key agreement protocol design. On one hand, HAAT enforces strict Source sensor access manage to cope with mutually free riders and spiteful Source sensors. On the other hand, HAAT offers complicated Source sensor privacy protection against both adversaries and different other network entities.

REFERENCES

[1] C. E. Perkins, Ad Hoc Networking. New York: Addison-Wesley, 2001.

[2] H. Yang, et al., “Security in Mobile Ad-Hoc Wireless Networks: Challenges and Solutions,” IEEE Wireless Comm. Magazine, Feb 2004.

[3] Y. Challal, H. Bettahar and A. Bouabdallah, "A taxonomy of multicast data origin authentication, issues and solutions,"IEEE Comm. Surveys and Tutorials, Vol. 6, No. 3, pp. 34-57, 2004.

[4] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels." Proc. of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.

[5] M. Youssef, A. Youssef and M. Younis, "Overlapping Multihop Clustering for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed systems, to appear (a preprint is accessible at http://doi.ieeecomputersociety.org/10.1109/TPDS.2009.32).

[6] J. Y. Yu and P. H. J. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, Vol. 1, No. 1, pp. 31-48, 2005.

[7] D. Balfanz, et al., "Talking to strangers: Authentication in ad-hoc wireless networks," Proc. of the Network and Distributed System Security Symposium (NDSS'02), San Diego, California, Feb 2002.

[8] R. Canetti et al., "Multicast Security: A Taxonomy and Efficient Constructions," Proc. of INFOCOM'99, New York, NY, March1999.

[9] R. Safavi-Naini and H. Wang, "Multi-receiver Authentication Codes: Models, Bounds, Constructions, and Extensions," Information and Computation, Vol. 151 No. 1-2, 25 pp. 148-172, May 1999.

[10] Perrig, et al., "Efficient and Secure Source Authentication for Multicast," Proc. of the Network and Distributed System Security Symposium (NDSS'01), San Diego, CA, Feb 2001.

[11] A. Perrig, "The BiBa One-time Signature and Broadcast Authentication Protocol," Proc. of the 8 th ACM Conf. on Computer and Communication Security, Philadelphia, PA, Nov 2001.

[12] L. Reyzin and N. Reyzin, "Better than BiBa: Short One-time Signatures with Fast Signing and Verifying," Proc. 7 th Australian Conf. on Info. Security and Privacy (ACISP'02), LNCS Vol. 2384, pp. 144-153, 2002.

[13] A. Savvides, C. C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-hoc Networks of Sensors," in theProceedings of the MOBICOM'01), pp. 166–179, Rome, Italy, July 2001.

[14] The Network Simulator - ns-2(http://www.isi.edu/nsnam/ns/).

[15] Younis, M.; Farrag, O., "Tiered Authentication of Multicast Traffic in Wireless Ad-Hoc Networks," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1,7, Nov. 30 2009-Dec. 4 2009; doi: 10.1109/GLOCOM.2009.5425260

[16] C.K. Wong, M. Gouda, and S. Lam. "Secure group communications using key graphs". in Proceedings of ACM SIGCOMM. 1998.

[17]. Guevara Noubir, "Optimizing Multicast Security over Satellite Links". 1998, European Space Agency. 3. Guevara Noubir and L.v. Allmen. "Security Issues in Internet Protocols over Satellite Links". in Proceedings of IEEE Vehicular Technology Conference (VTC'99 Fall). 1999. Amsterdam, Holland.

[18]. Guevara Noubir, Feng Zhu, and A.H. Chan. "Key Management for Simultaneous Join/Leave in Secure Multicast". in Proceedings of IEEE International Symposium on Information Theory (ISIT). 2002.

[19]. Refik Molva and A. Pannetrat, "Scalable Multicast Security with Dynamic Recipient Groups". ACM Transactions on Information and System Security, 2000.

[20]. Suvo Mittra. "Iolus: A Framework for Scalable Secure Multicasting". in Proceedings of ACM SIGCOMM '97. 1997. Cannes, France.

[21]. Ran Canetti, et al. "Multicast Security: A Taxonomy and Some Efficient Constructions". in Proceedings of INFOCOMM. 1999: IEEE Press.

[22]. A. Perrig, D. Song, and D. Tygar. "ELK, a new protocol for efficient large-group key distribution". in Proceedings of IEEE Security and Privacy Symposium. 2001.

[23]. D. Balenson, D. McGrew, and A. Sherman, "Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization". 1999, Internet Draft.

[24]. D. M. Waller, E. C. Harder, and R.C. Agee, "Key Management for Multicast: Issues and Architectures". 1998, Internet Draft.

[25]. F. Zhu, A. H. Chan, and G. Noubir. "Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast". in Proceedings of MILCOM. 2003. Boston, MA, USA.

[26]. Guevara Noubir. "A Scalable Key Distribution Scheme for Dynamic Multicast Groups". in Proceedings of Third European Research Seminar on Advances in Distributed Systems. 1999. Madeira Island, Portugal.

[27]. S. Setia, S. Koussih, and S. Jahodia. "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast". in Proceedings of IEEE Security and Privacy Symposium. 2000. Oakland, CA, USA.

[28]. Adrian Perrig and D. Tygar, "Secure Broadcast Communication in wired and wireless networks". 2002: Kluwer.

[29]. Y. Yang, X. Li, and S. Lam. "Reliable Group Rekeying: Design and Performance Analysis". in Proceedings of ACM SIGCOMM. 2001. San Diego, CA, USA.

[30]. R. Poovendran and J.S. Baras. "An Information Theoretic Analysis of Rooted-Tree Based Secure Multicast Key Distribution Schemes". in Proceedings of Advances in Cryptology CRYPTO'99. 1999.

[31]. L. Gong and N. Sacham, "Multicast Security and its Extension to a mobile Environment". Wireless Networks, 1995. 1(3): p. 281-295.

[32]. Danilo Bruschi and E. Rosti, "Secure Multicast in Wireless Networks of Mobile Hosts: Protocols and Issues". Mobile Networks and Applications, 2002. 7: p. 503-511.

[33]. C. Zhang, et al. "Comparison of Inter-Area Rekeying Algorithms for Secure Wireless Group Communications". in Proceedings of Performance 2002. 2002. Rome, Italy.

[34]. Thomas Kostas, et al. "Key Management for Secure Multicast Group Communication in Mobile Networks". in Proceedings of DARPA Information Survivability Conference and Exposition. 2003.

[35]. Loukas Lazos and R. Poovendran. "Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information". in Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing. 2003. Hong Kong, China.

[36]. Yih-Chun Hu, Adrian Perrig, and D.B. Johnson. "Efficient Security Mechanisms for Routing Protocols". in Proceedings of Network and Distributed System Security Symposium. 2003.

[37]. B. Dahill, et al., "ARAN: A secure Routing Protocol for Ad Hoc Networks". 2002, UMASS Amherst.

[38]. P. Papadimitratos and Z. Haas. "Secure Routing for Mobile Ad Hoc Networks". in Proceedings of CNDS. 2002.

[39] L. Buttyan and J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks". ACM/Kluwer Mobile Networks and Applications (MONET), 2003. 8(5).