Group-Key Management Model for Worldwide Wireless Mesh Networks

Saurav Ghosh[1], Subir Bhadra[2], Indrajit Bhattacharya[3]
A.K Choudhury School of I.T
University of Calcutta
3Kalyani Govt. Engg. College, West Bengal University of Kalyani.
E-mail : sauravghoshcu@gmail.com, bhadra.subir@gmail.com, indra51276@gmail.com

Abstract*— Wireless Mesh Network (WMN) is an upcoming wireless network technology and is mainly used to provide broadband internet in remote locations. It is characterized by minimum fixed infrastructure requirement and is operated in an open medium, such that any user within the range covered by mesh routers may access the network. So a critical requirement for the security in WMN is the authentication of users. However, WMN is far from mature for large-scale deployment in some applications due to the lack of the satisfactory guarantees on security. A well-performed security framework for WMN will contribute to network survivability and strongly support the network growth or reduction. A key management model to overcome the scalability issue on security aspect for large-scale deployment of WMN i.e. Worldwide WMN is proposed in this work, which aims to guarantee well-performed key management services and protection from potential attacks. Here, we use a combination of techniques, such as zone-based topology structure, off-line CA, virtual certification authority) etc.

***Index Terms*—WWMNs, PKG, Strata, DSR**

I. INTRODUCTION

Fig.1 describes a typical infrastructure of a WMN model. Now with the future large-scale deployment of worldwide wireless connection, group communication is a very important pattern in WMNs [1, 2]. Securing group communication in dynamic and large-scale groups is more complex than securing one-to-one communications due to the inherent scalability [9] issues of group key management.

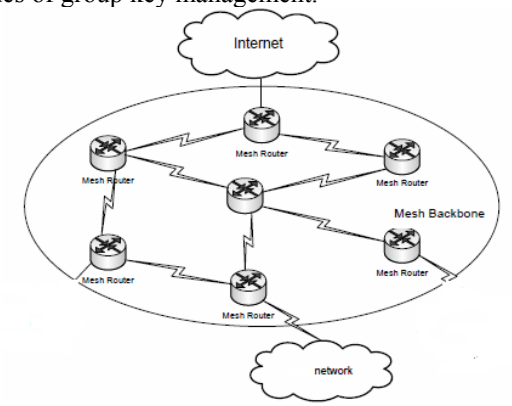

Fig. 1: A typical infrastructure of WAN

When we want to focus on **worldwide wireless connection** through WMNs it is obvious the size of the mesh backbone is huge. In our proposed model (zone-based network model [10]) we addressed the scalability [9] issue by partitioning the Mesh Backbone/ Backbone networks/ Backbone routers (Fig.2) into different strata or segment or group depending upon the geographical region such that it makes each stratum relatively independent. Here R_i s are the different strata/region/group for all i=1 (1) p.

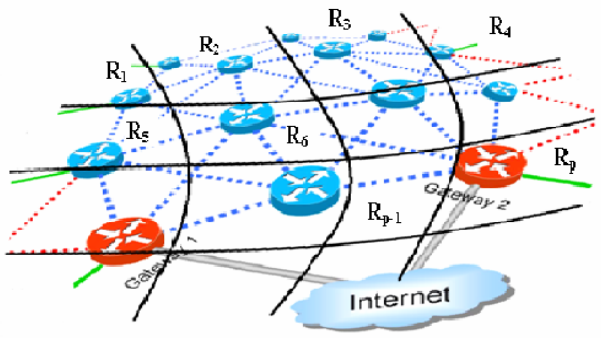

Fig.2: Zone-based Wireless Mesh Network model.

II. SECURITY CHALLENGES IN WMNS:

There are many security issues in WMNs viz. Secure Routing, Secure Location information, Authentication & key management etc. Due to the fundamental importance, we have initially focused on Authentication & key management with the expected outcome of a low-computational and scalable key management framework with well-performed security functions and protection from potential attacks. After that we have extended our concept over WWMNs.

A. Authentication & key management:

In wireless networks, authentication is very important because of the shared nature of the wireless medium. Any node, legitimate or malicious, with a suitable hardware device can send data into the network.

Verifying that the data received is from a legitimate entity is critical for securing the network. In this aspect, the public key infrastructure (PKI) [7] and certification authority (CA) provide two important mechanisms for authentication.

Authentication is usually realized by implementing PKI based on asymmetric cryptography in which each user has a pair of cryptographic keys: public key and private key. The public key is widely distributed and known by all the users while the private key is only secretly kept by the user. One property of the pair of keys is that a message encrypted with the public key can only be decrypted with the corresponding private key and vice versa. By exploiting this, authentication can be achieved. For instance, a sender can digitally sign the packets using its own private key before sending them. If the receiver can successfully decrypt the messages with the sender's public key, it is assured that the packets are really sent by the claimed sender rather that someone else.

So, to check the validity of a digital signature, it is necessary to first verify that the sender's public key does belong to the sender, which requires a Certificate Authority (CA) be involved in the authentication procedure. The CA signs the binding of an entity's identity and its public key with its private key, and issues the signature as the entity's certificate. Any entity can validate the binding of sender's identity and public key by checking its certificate using CA's public key. A node may update its certificate periodically to reduce the chance of brute-force attack on its private key. So the CA has to stay on-line to reflect the periodically changing certificates. This scheme is based on the following assumptions:

- the CA's public key is known by every entity in the network,
- the CA's public key and signed certificates are globally trusted in the network, and
- the communication channels through which the entities get other's certificate from CA are secure.

However, the absence of pre-established trusted network infrastructure in WMNs obstructs direct application of PKI. This is because it is impractical to deploy a CA that every node can trust and establish a secure communication channel with. A distributed CA scheme is thus required.

B. Distributed CA:

A distributed CA scheme will be used instead of centralized CA to utilize the applications of PKI which is the most common practice in key management. Distributed CA distributes the functionality of the centralized CA to the whole network by applying threshold cryptography [4] which has been proved efficient and well-performed.

C: Scalability and Security Issue on WWMNs:

In this work, we are trying to consider the scalability issue along with the security issue on WWMNs [9], where the 'Scalability' is a desirable property of a system, a network, or a process, which indicates its ability to either handle growing amounts of work in a graceful manner, or to be readily enlarged [5].

III. SYSTEM INITIALIZATION AND NECESSARY COMPUTATION:

Before assigning an authorized certificate and an authorized key to a user, the system completes the following initialization steps:

(a) Every region/strata/group R_1, R_2,……,R_p has a centralized CA, say CC_1, CC_2, ……, CC_p, say Combiner-checker [8, which are the special type of routers, have the ability of two types of communication viz. wireless and wired.

(b) Within the region/zone it (CC_i) acts as wireless but among the regions they have wired communication.

(c) The every CA creates two pairs of private and public keys, one for itself and the other one for the regional system using some (may be RSA) algorithm. The public key for the i^{th} regional system is denoted as K_i and its corresponding private key as P_i.

(d) Before accessing a regional/stratum network, every terminal user must register with its CA. If a terminal user wants to serve as a regional/stratum router, the terminal user must submit an application to the CA of that region besides its user information. If the terminal user is approved of being a backbone or regional router, the CA would confirm it as a backbone or regional router. Every user broadcasts its user ID to all other users.

(e) N_i be the total no. of backbone routers in the i^{th} region/strata/group such that

$$\sum_{i=1}^{p} N_i = N \text{ ----------(1)}$$

where N is the total no. of backbone routers in the networks.

(f) n_i is the no. of backbone routers selected from the i^{th} segment/region/strata, such that

$$\sum_{i=1}^{p} n_i = n \text{ ----------(2)},$$

where n is the total no. of selected routers from all the strata.

(g) Every regional CA would select n_i terminal routers from i^{th} region with suitable procedure, viz. $\mathbf{BR_{ij}}$, for all i=1(1)p and j=1(1)n_i, which serve as private key generation (PKG) nodes within the region/strata/group. But [6] described this $\mathbf{BR_{ij}}$ as "**higher performance**" routers which have almost no significance to construct the PKG. These n_i backbone routers would then form a virtual CA of the ith region and manage the keys using the (x_i, n_i)- threshold cryptographic method [8]. That is, the CA publishes the public key K_i of that region to all of its users while the private key P_i of that region is partitioned into n_i pieces $P_{i_1}, P_{i_2}, \ldots\ldots\ldots, P_{i_{n_i}}$ and assigns the n_i pieces to the n_i different backbone routers. Any t_i out of the n_i backbone routers could reconstruct the private key P_i. Therefore, any m_i out of the n_i backbone routers cannot reconstruct private key P_i unless $m_i \geq x_i$.

There must be a proper procedure to define the size of the PKG. In this work we mainly concentrated on this size selection process.

(h) Y_{ij} s are the physical distance between j^{th} router of i^{th} strata/group and its CA (CC_i), for all i=1(1)p and j=1(1)N_i.

(i) $$\bar{Y}_{N_i} = \frac{1}{N_i}\sum_{j=1}^{N_i} Y_{ij} \text{ ----------(3)},$$

mean distance in the i^{th} stratum.

(j) $$\bar{Y}_N = \frac{1}{N}\sum_i\sum_j Y_{ij} = \frac{1}{N}\sum_{i=1}^{p} N_i \bar{Y}_{N_i} \text{ ----------(4)},$$

mean distance of the whole backbone network.

(k) $$S_i^2 = \frac{1}{N_i - 1}\sum_{j=1}^{N_i}(Y_{ij} - \bar{Y}_{N_i})^2, i = 1(1)p \text{ ----------(5)},$$

is the population mean square of the i^{th} stratum.

(l) y_{ij}= value (distance) of the j^{th} selected router of the i^{th} stratum.

(m) $\bar{y}_{n_i}$ Mean distance of the selected router from the i^{th} stratum.

(n) $$s_i^2 = \frac{1}{n_i - 1}\sum_{j=1}^{n_i}(y_{ij} - \bar{y}_{n_i})^2, i = 1(1)p \text{ ----------(6)},$$

is the mean square distance of the selected unit from i^{th} stratum.

(o) Estimate of the population mean ($\bar{Y}_N$) from selected sample using:

$$\bar{y}_{st} = \frac{1}{N}\sum_{i=1}^{p} N_i \bar{y}_{n_i} \text{ ----------(7)},$$

(p) $$\text{var}(\bar{y}_{st}) = \frac{1}{N^2}\sum_{i=1}^{p} N_i(N_i - n_i)\frac{S_i^2}{n_i} \text{ ----------(8)},$$

and its estimate is given by

$$\text{Est}(\text{var}(\bar{y}_{st})) = \sum_{i=1}^{p}\frac{N_i^2}{N^2}.\frac{s_i^2}{n_i} \text{ ----------(9)}.$$

Thus it may be observed from Equ.(9) that $\text{Est}(\text{var}(\bar{y}_{st}))$ depends on s_i^2 i.e. how far the samples are deviated from its mean distance within the segment/region/strata. Thus, if s_i^2, are small then the $\text{var}(\bar{y}_{st})$ is small and hence the total time to distribute the CA's information to its distributed/virtual CAs is small.

Another important observation is that $\text{var}(\bar{y}_{st})$ is also depending on n_i, size of the selected sample from the ith segment/region/strata and hence we are concentrated on selection process of the different value of n_i for different segment.

IV. SELECTION PROCESS AND ITS OPTIMIZATION:

A. Proportional Selection:

Scalability (network being adaptable and expandable) problem can be solved by 'Proportional selection' process,

$$n_i \propto N_i ,$$

i.e. if N_i increases then n_i must be increased. Here we can say that if N increases/decreases over time, then we have to increase/decrease n as desire, so as to $\frac{n}{N}$ = constant(c), and hence

$$\frac{n_i}{N_i} = c = \frac{n}{N} \text{ ---------- (10),}$$

B. Periodic Selection & its Optimization:

In our above describe selection process there is no concept of time constraint. Here we want to introduce a new selection process which includes the time constraint. Let us assume that, refresh the selection process after every T time-unit, so that the scalability issue can be overcome in real life scenario.

So here we introduce the "Stratified" selection process. Let, the time function T in this stratified selection has the following form

$$T = a + \sum_{i=1}^{p} t_i n_i \text{ ---------- (11),}$$

where 'a' is a constant and 't_i' is the average time required to select per unit in the ith segment/group/stratum for all i=1(1)p.

So our problem converts to as below:
"We have to select the value of n_is from different segment after every T time-unit interval such that $var(\bar{y}_{st})$ is minimum and hence precision will be maximum i.e. time required to distribute the CAs information to its distributed/virtual CAs is minimum".

Hence we have to minimize $var(\bar{y}_{st})$ subject to the condition

$$\sum_{i=1}^{p} t_i n_i = T - a \text{ ---------- (12).}$$

Eventually we have to minimize

$$\psi = var(\bar{y}_{st}) + \lambda\left(\sum_{i=1}^{p} t_i n_i - T + a\right) \text{ ---------- (13),}$$

Unconditionally for variation in n_i and λ being Lagrange's multiplier.

Substituting the value of $var(\bar{y}_{st})$ from (8) we have

$$\psi = \frac{1}{N^2}\sum_{i=1}^{p} N_i(N_i - n_i)\frac{S_i^2}{n_i} + \lambda\left(\sum_{i=1}^{p} t_i n_i - T + a\right) \text{ ------ (14).}$$

Differentiating ψ partially w.r.t. n_i and equating to zero, we get for an extremum

$$n_i = \frac{N_i S_i}{N\sqrt{t_i \lambda}} \text{ ---------- (15).}$$

Summing both sides of (15) over i from 1 to p, we get the $\sqrt{\lambda}$ and substituting this value in Equ.(15) we get

$$n_i = \frac{nN_iS_i / \sqrt{t_i}}{\sum_{i=1}^{p}[N_iS_i / \sqrt{t_i}]} \text{ ---------- (16).}$$

Thus, in optimum selection for a fixed time

$$n_i \propto \frac{N_iS_i}{\sqrt{t_i}} \text{ ---------- (17).}$$

From Equ.(17), the following conclusions can be made: A large sample (the value of n_i) would be required from a group if

- Segment/group/stratum size(N_i) is large,
- Segment/group/stratum variability(S_i) is large,
- Time requires for selecting every unit is low in the group.

From equation (16), it can be observed that n_i is given in terms of n. The value of n depends upon whether the sample is elected so as to meet a specified total time T.

For a fixed time T, substituting from equation (16) in time function equation (11), the optimum total sample size n is given by

$$n = \frac{(T - a)\sum_{i=1}^{p} (N_i S_i / \sqrt{t_i})}{\sum_{i=1}^{p} N_i S_i \sqrt{t_i}} \text{ ----------(18).}$$

In particular if $t_i = t_0$, $\forall$ i=1 (1) p, then we have the following consequences:

$$n_i = n \frac{N_i S_i}{\sum_{i=1}^{p} N_i S_i} \text{ ----------(19).}$$

Hence the optimum value of n_i, is in Equ.16 or in Equ.19 and by using it, maximize the required precision.

V. WORLDWIDE ISSUE.

In particular, the high computation overhead for key establishment and key renewing i.e. selecting distributed CAs is usually relevant to the group size and consequently becomes a performance bottleneck in achieving scalability [2] for Worldwide WMN. According to our model we can thrash this issue as below:

A: Different Regions/ Strata selection:

Suppose client A of region R_i want to communicate with client B of region R_j (Fig. 3). According to some routing protocol (may be DSR or AODV) the selected path ( ) passes through the regions R_i, R_5, R_6, R_2, R_3, R_j for this communication. It is clear from the Fig. 3 that, we have not incorporated all the regions of the entire network, we only consider R_i, R_5, R_6, R_2, R_3, R_j regions.

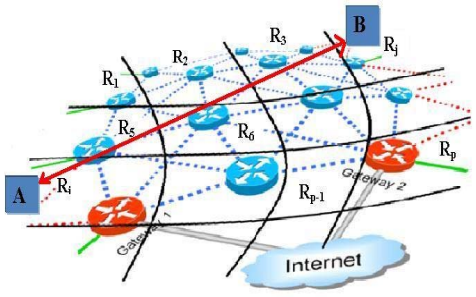

Fig. 3: Client A communicates with client B

B: Application of TC over the proposed model:

Now the new backbone network size, N_{new}=total no. of routers from the selected regions is obviously less than N. Accordingly the new value of total selected sample routers n_{new} (calculate using Equ.(18)), is also obviously less than n. And now we can calculate the values of n_i s of the selected regions using either Equ.(16) or Equ.(19). The n_i backbone routers would form a virtual CA and manage the keys using the (x_i, n_i)-threshold cryptographic method [8] for every selected i^{th} region separately as discussed previously.

a. Proposed Authentication algorithm for WWMNs:

Let us consider our example as in Fig. 3 i.e. communication takes place between client A of region R_i and client B of region R_j through the regions R_i , R_5, R_6, R_2, R_3, R_j and the corresponding algorithm as given below:

Assume all the public keys of CC_i s are known to each other for all i=1(1)p.

BEGIN

Step I: Set $FLAG_A = 0$.

Step I.I: Message 'm_A' containing A's identity, its public key, its regional ID, the ID of the destination region and the destination client and signed by x_i no. of nodes/ virtual CAs and generate x_i no. of partial signatures as $PS(m_A, P_{i_1}), PS(m_A, P_{i_2}), \text{-------}, PS(m_A, P_{i_{n_i}})$.

Forward these partial signatures to the regional CA, called 'combiner-checker' [8] 'CC_i' and generates the certificate CR_i. Now 'CC_i' checks whether CR_i is the same as it is signed by CA's private key P_i. So, 'CC_i' actually checking whether any x_i out of n_i backbone routers virtual CAs could reconstruct the private key P_i (Fig. 4).

Step II: If the above try of 'CC_i' fails to authenticate then stop the process immediately and try the process again with another set of x_i routers to construct the CR_is .

Step III: This trail-error process continuesτ no. of times at most for very region/zone.

Step IV: If any success occurs in Step II or in Step III

Set $FLAG_A = 1$.

Else

Terminates the communication as authentication fails i.e. go to **END**.

Step V: The CA, CC_i' will construct a message 'M_A', which contains $FLAG_A$ =1 and CR_i and M_A is encrypted with CC_i 's private key.

Step VI: Now CC_i will check whether B is under it's region or not?

Step VII: If the answer of Step VI is false then
Transfer the message 'M_A' to the next region's Combiner-Checker (as CC_5 in our example) and follow the Step VI.
Else if the answer of Step VI is true then
Combiner-Checker asks the destination client to prove its own authentication using Step I to Step IV.

Step VIII: Finally if the 'Else if'-part in Step VII is occurs successfully then
The proper authentication (decrypt the M_A using CC_i's public key which is known to CC_j) as well as proper communication has been established between source and destination client (Fig. 4).

END.

b. Pictorial representation of authentication process in WWMNs

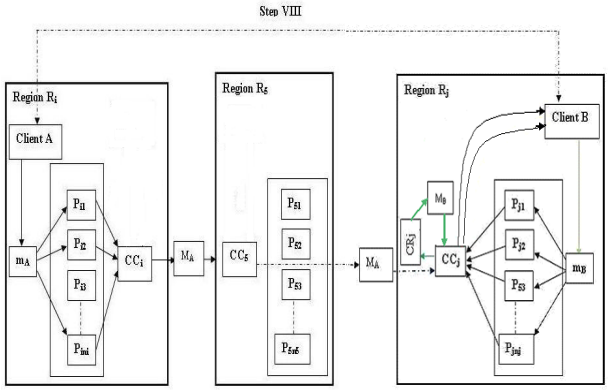

Fig. 4: Pictorial Representation of authentication process in WWMNs

VI. SIMULATION RESULTS

We have simulated our work in two parts as below using JAVA and C language:

- Detecting the value of PKG / virtual CA (n_i) for each region using 'zone-based selection' and 'proportional selection', respectively.
- Detecting the communication path using DSR technique for our proposed 'zone-based WWMNs' algorithm and non-zone-based WWMNs.

A: Detecting the value of PKG / virtual CA (n_i)

The simulated parameters are listed in Table 1.

Parameters	Values
No. of regions	15
Total no. of routers (N_i) /zone	Randomly generated and it is > 8 and < 400
Physical distance of every node from its CC_i	Randomly generated
Average time to select a node by its CC_i for each 15 regions	Times in milliseconds
Network refreshment time	300000 ms.
Constant value by which proportional selection is possible	0.015

Table1: Simulation parameters for PKG / virtual CA (n_i)

At the beginning of the simulation, randomly generate total no. of routers (N_i) for each region and also randomly generate the physical distance to each node from its CC_i. Now we conduct this simulation 20 times consecutively.
Fig.5 represents the 20 pairs of n values ($n = \sum n_i$, i=1(1)15), which are obtained by simulating using two diff. methods.

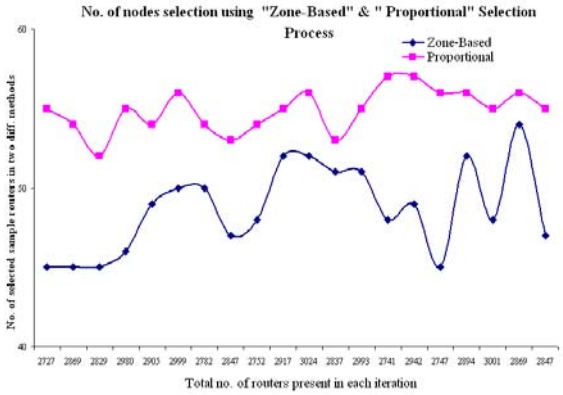

Fig. 5: No. of nodes selection using "Zone-Based" & "Proportional" Selection Process

From the simulation it was found that the average PKG sizes are 54.9, 48.7 for "Zone-Based" & "Proportional" selection respectively. So, the average gains per simulation in zone-based over proportional selection is 6.2. In 24 hours 288-times refreshment is required @ 5min. interval and hence the group-based selection selects 6.2*288=1788 less sample than proportional

selection, which is a immense gain in terms of time constraint as well as mathematical computations.

B: Detecting the communication paths using DSR technique

For this part of simulation the parameters are as in Table 2.

After all the assignment has made for all the parameters, simulations have been done for 20 pair of communicating nodes. Fig.6 shows the no. of hop counts for two different methods of communication.

Parameters	Values
No. of zones/regions	7
No. of nodes per zones	5,7,6,7,6,7,7 respectively
CC_i for each zone	Node E, M, V, Z, p, I, v respectively
Physical distance among all CC_i s	Assign the distance randomly
'Radio range index 'among all nodes zone-wise	Assign it randomly
'Radio range index ' for all nodes of the whole network	Assign it randomly
Communicating nodes	Take two nodes randomly

Table 2: Simulation parameters for path selection

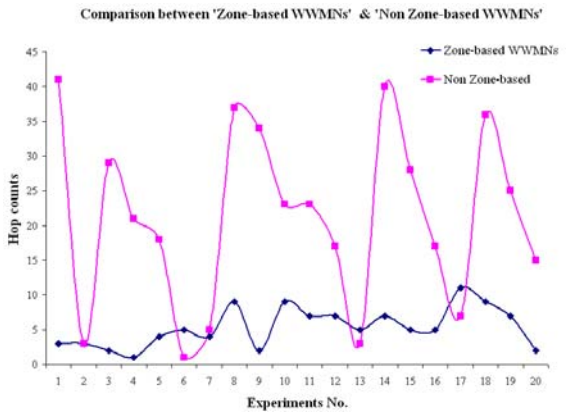

Fig.6: Hop counts between two node communication for 'Zone-based WWMNs' & 'Non Zone-based WWMNs'

From the simulation results we can calculate the %coefficient of variation (%CV) for both the distribution and that are 52.61 and 60.63 for 'zone-based' and 'non zone-based'. So, on-an-average the gain is 8% in terms of hop counts to communicate between two randomly chosen nodes.

VII. Conclusion and Future Work

(a) Now the question is after what time we should re-evaluate the sample size n_i?

Assume that this process continues τ_i number of times for i^{th} region. And also suppose that, the time required to complete this process, n_i number of times, for i^{th} particular region is time- unit such that,

$$\xi_i \le \tau_i x_i t_i,$$

i=1(1)2*, where 2* total no. of selected region/zone where the actual authentication process occur according to our routing protocol, and hence

$$\sum_{i=1}^{2} \xi_i + \delta \le T,$$

where δ is a constant time required for intermediate passing .

(b) So in this way it may be concluded that after at most $\sum_{i=1}^{2} \xi_i + \delta$

,time-units interval the sample size n_i should be re-evaluated such that the scalability problem can be solved.

(c) This sequential authentication process may require less time to complete than an unorganized process because it requires less no. of computation works.

(d) The use of time function with minimum variability in the zone-based selection is essential over the proportional selection, where there is no concept of minimization of variance with the time function.

(e) This work only represents the initial effort for the development of a sophisticated authentication scheme for Worldwide Wireless Mesh Networks (WWMNs). This work has been projected a low-computational and scalable key management model for WWMNs which aims to guarantee well-performed key management service and protection from possible attacks.

(f) As the future work towards achieving the ultimate goal, it is needed to do more quantitative analysis using a WMN test bed. We will plan to combine our two diff. simulations process on that test bed.

Acknowledgment

Author† sincerely acknowledge the contribution of the faculty members and technical support staffs of CSE Dept. and also thankful to the management of MCKV Institute of Engineering, Liluah, Howrah.

References

[1] F Lee and S. Shieh, "Scalable and Lightweight Key Distribution for Secure Group Communications,"

International Journal of Network Management, 14:167-176, 2004.

[2] Y. Fu, J. He, R. Wang and G. Li, "A key-chain-based keying scheme for many-to-many secure group communication," ACM Transactions on Information and System Security (TISSEC), 2004, vol. 7(4), pp. 523 – 552

[3] S Mittra, "Iolus: a framework for scalable secure multicasting," in Proceedings of ACM SIGCOMM'97, Canada, September, 1997, pp. 14-18.

[4] Y. Desmedt, "Threshold cryptography," European Transactions on Telecommunication, vol. 5(4), 1994. pp. 449-457.

[5] M S. Siddiqui, and C. S. Hong, "Security Issues in Wireless Mesh Networks", Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07). New York IEEE Press, 2007, pp.41−47.

[6] Yingfang Fu, Jingsha He, Rong Wang2 and Guorui Li, "Mutual Authentication in Wireless Mesh Networks" proceeding of ICC, 2008.

[7] W. Zhang, Z. Wang, S. K. Das, and M. Hassan, Chapter 12 - "Security Issues in Wireless Mesh Networks" in the book "Wireless Mesh Networks Architectures and Protocols".

[8] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, p. 24-30, 1999.

[9] Li Gao, Elizabeth Chang, Sazia Parvin, Song Han, Tharam Dillon, "A Secure Key Management Model for Wireless Mesh Networks" 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[10] Mihail L. Sichitiu, "Wireless Mesh Networks: Opportunities and challenges", Proceedings of the Wireless World Congress, (Palo Alto, CA), May 2005

[11] Ferreira, E.W.T.; de Oliveira, R.; Carrijo, G.A.; Bhargava, B.; "Intrusion Detection in Wireless Mesh Networks Using a Hybrid Approach" Distributed Computing Systems Workshops, 2009. ICDCS Workshops '09. 29th IEEE International Conference

[12] Yatao Yang, Ping Zeng, Xinghua Yang, Yina Huang "Efficient Intrusion Detection System Model in Wireless Mesh Network" ; Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference