Security Enhancement in DPKG for IBC Using Intrusion Detection Systems in MANET

B. Asha Devi[1] (PG scholar), Mr.A.Jegatheesan[2] (Head dept of IT)

[1]PG Department of Computer Science and Engineering, [2]Department of Information Technology

Cape Institute of Technology, Levengipuram

Anna University Chennai

ABSTRACT—Key distribution and security are the essential requirement in MANETs. In our paper we are using intrusion detection nodes to monitor and detect the malicious activities as well as finding the best node to select as PKGs based on security and energy constrains. Instead of selecting a single node as PKG, selecting t nodes using intrusion detection systems and the PKG task is distributed among these nodes using DPKG protocol. We are using intrusion detection nodes as a filter for enhance the security, increase network lifetime, preventing the self organization nature.

Keywords— MANET, entity authentication, distributed private key generation, verifiable secret sharing, PKG, Intrusion detection system.

I. INTRODUCTION

Key distribution and security are the essential requirement in MANETs. In IBC the private key is generated and distributed by a offline centralized server called private key generator. But in ad hoc network finding the offline centralized server is not possible and the centralized server must be a trusted party otherwise the secret get be loosed because the PKG is one and only responsible for generating and distributing the private key. In our paper this key generation involves two step. In first step the selection of a secure node based on the security and energy level using intrusion detection nodes is performed. In the second step this DPKG protocol [1] is get implemented. A.Karygiannis *et al* proposed the security monitoring is performed only at the main points to be encountered in a temporary network, and an approach provides conservation of limited resources [5].

This PKG task is get distributed among all the nodes in the network by using the protocol called distributed private key generation (DPKG).This is mainly based on Feldman verifiable secret sharing scheme. The secret is divided and distributed among t nodes. When a node want to communicate with other nodes it first want to get the entire share through the Feldman verifiable secret sharing scheme [2]. Kate *et al.* [3] also proposed distributed private key generators for identity based cryptography, in which generalized construction is given, which actually antedates [3]. Farzaneh Pakzad [6] presents various intrusion detection techniques to detecting the malicious nodes in the distributed ad hoc network. Vinay P.Virada presents various type of intrusion detection system, their architechure, different type of attacks [7]. In novel based Intrusion detection architecture the monitoring is performed based on an event happens in the network is proposed at ETBAS. The dynamic node selection process is critical as a stochastic problem, and selecting the optimal nodes based on the security conditions and energy states as PKGs from all available nodes [4].In our paper we combining the best approaches found in [1] and [4] to enhance the security in

distributed private key generation and improving the network lifetime.

II. Security Enhancement In DPKG For IBC Using Intrusion Detection Systems In Manet

In this section, we first introduce some basic preliminaries of intrusion detection systems, insider thread, attackers, and the problem in selecting the best node to function as aPKG.And we give our proposed work that consist of two steps in first step we discuss about the initial node selection to function in PKG process using intrusion detection systems and describe how they are working as filter for detecting the attackers nodes in MANETs. During the second step the task of private key generation is distributed among the selected PKG nodes using the DPKG for IBC protocol. Each node has different identity. Again this DPKG protocol for IBC proposed by Chan [1] is briefly discussed, that consist of two phases first phase consist of distributed key generation and second phase deals with threshold private key extraction. Our proposed model efficiently enhances the security in key generation and distribution for MANET. And they efficiently and securely perform the key generation in the distribution manner against the attacks like DoS, impersonation, malicious attacks.

2.1 Intrusion Detection System

An illegal act of entering, seizing, or taking possession of another property or a wrongful entry after the determination of a particular estate is the illegal activities. These illegal activities degrade the network performance, fully drain the energy resources, make vulnerable to the security and confidentiality of the network. These illegal activities are called intrusion.

A system used to detection of such activities as malicious activities by monitoring the nodes and take the necessary action as response to the detected malicious activities is called intrusion detection systems.

The data collection component is responsible for collection of data for different sources the sources may be homogeneous or heterogeneous sources. In the detection component the collected data is analysed to detect intrusion attempts and indications of detected intrusions are sent to the response component.

Anomaly-based intrusion detection store the history of symptoms of normal behaviours of the node as a description such as Energy usage, resource usage etc... The nodes whose behaviour is deviated from the normal behaviours that node is detect as an unauthorized node or an malicious node and send the alert to the responding node. Misuse based intrusion detection perform the comparison of known attack signatures with current system activities. But the drawback is, it cannot able to detect the new attacks entered currently in the network. set of constraint are specified in the program or protocol as a basic constraint that each node should be satisfied if any node that should not satisfying this constrain then that node detected as intrusions and these intrusions are detected as run time violations this is called specification based intrusion detection. Once the intrusions are detected it should be notified to the appropriate authorized node.

2.2 Attacks

In general attacks can be classified in to two types they are Active attack and passive attack. Passive attacks are refer to the attempts made by malicious node to perceive the nature of activities and to obtain information transacted in the network without disrupting the operation. Active attacks disrupt the operation of network. Nodes that perform internal attacks are compromised nodes. In our paper we are enhancing the security in distributed private key generation by avoiding such malicious attack using the intrusion detection nodes.

IDs periodically monitor the nearby nodes and detect the nodes under the malicious attack such it avoid the selection of nodes already under the attack or avoid the selection of compromised node to function in the PKG process. Our proposed work efficiently and improve the network performance, life time by avoiding such attacks given below.

2.2.1 Denial of service

The attack processed by making the network resources unavailable for service to other nodes, either by consuming the bandwidth or overloading the system.

2.2.2 Resource consumption

The scarce availability of resources in the ad hoc wireless network makes it an easy target for internal attacks. In these type of attacks one of the major type is , Energy depletion —The aim of this type of attacks to depleting the energy level of the critical nodes.

2.2.3 Host Impersonation

A compromised internal node can act as authorized node and respond with fake control packets to create wrong entries. It will cause the security vulnerability in the mobile ad hoc network.

2.2.4 Information disclosure

A compromised node can act as an informer, that deliberate disclosure of confidential information to the unauthorized nodes. Selection of such node to function in the PKG process causes the critical situation, vulnerabilities in the network.

In our proposed system IDs are used to select the best node to function in the PKG process, this selection is done based on the constrains energy level and security state. Low energy level nodes are not selected. Node with high rank only selected for this process.

2.3 Insider Threat

An insider threat is a type of malicious attack it also may be hacker or black hat who is an participant or agency in the network. An outside person or an unauthorized user can poses as a participant or authorized user by obtaining false evidence of authority. The cracker obtains access to the targeted networks and then conducts illegal activities that cause harm to that network. The malicious activity usually occurs in four steps or phases. First, the cracker gains entry to the system or network. Secondly, the cracker investigates the nature of the system or network in order to learn where the vulnerable points are and where the most damage can be caused with the least effort. Thirdly, the cracker sets up a workstation from which the nefarious activity can be conducted. Finally, the actual destructive activity takes place

The result of inside threat are viruses, worms, Trojan horses, the theft of secrets, the corruption of secret data, the modification of data to produce trouble or erroneous criminal evidence. Multiple use of spyware, anti-virus, firewalls, are used for detecting this malicious activities. In our paper we are using Intrusion detection systems to monitor periodically and report the detected malicious activities to the respond able person and performing the priority indexing of the neighbor nodes based on the rank which based on the constrains like security and energy level.IDs selecting the best node to function as PKG using the table lookup.

2.4 PKG selection using Intrusion detection systems

In distributed key generation the t PKG nodes jointly compute the private key of the private key generator and generate the corresponding public key. Each member has a share of the private key, if a node want to know about its private key first it want to obtain t share from t founding member perform the check on the received share and construct its private based on the nodes ID.

The founding members must be an trusted parties because share of the secret is generated and maintained by that nodes only. The private key generation task is distributed among all this t nodes. This t nodes act as a group PKG, the selection of each PKG node should be performed very carefully and as well as in a secure manner. The one of the best solution is to select the optimum nodes in the network to function as PKGs.

In general MANETs are distributed in nature, so the security state of the nodes in network can change dynamically; some of the nodes may be in a safe state and the remaining nodes may be under attack or may be compromised by enemies. Apparently, if we are selecting a compromised node as a PKG or a node already under an attack to function in the private key generation process would cause a thread to the security in the ad hoc network.Compromised nodes may deliberately relay bogus information in order to become selected as a member of the PKG. Therefore, leaving the node selection to be processed in IDs would be more secure and reliable. IDs do not hold any keys.

In addition, these IDs could be distributed in nature and periodically monitors each node's activities, comparing them with stored normal profiles in order to detect intrusions. The IDs performs a priority index table

lookup to find the best nodes based on current states of all available nodes.

Therefore, when constructing the PKG, it would be very sensible to consider the security state and energy level of the nodes in order to improve network lifetime and functionality in overall. These IDs can be distributed in nature and periodically monitors each node's activities, comparing them with stored normal profiles in order to detect intrusions.

In our proposed system, the IDs takes on the additional role of selecting the best node(s) to act as a PKG based on the reported security and energy conditions. In order to keep the security and energy information current, the system time can be divided into slots that correspond to the time intervals.

2.5 DPKG for IBC implementation

In this we describe about the distributed private key generation for identity based cryptosystems protocol proposed by Chan [1].This DPKG consists of two phases they are distributed key generation (DKG) and threshold private key extraction (TPKE). In the first phase, the members selected by intrusion detection systems (IDs) of an ad hoc group jointly compute the private key x of the PKG and publish the corresponding public key. In the next phase, each new coming member with an identity ID or member that want to communicate with others needs to obtain the shares from a sufficient t number of members selected by IDs of the group in order to construct his private key for ID Note that this share is only for constructing the private key of ID and has nothing to do with the shares of PKG's private key held by the members. Besides, only members that selected by IDs could generate a share and other members do not have the rights to generate the share. it is possible to differentiate between a member selected by IDs and a member who has joined afterwards.

2.5.1 Distributed Key Generation

Assume there are n nodes: $P1$, $P2$, . . . ,Pn. Assume that the bilinear pairing of the associated group is exist are. Let them be G1 and G2 of order q, that is, the pairing is ê: G1×G1 → G2. A Hash function H is used to map an identity ID ϵ {0, 1} $*$ to G1. The DKG construction is run parallel to the Feldman's verifiable secret sharing scheme. Each user Pi picks a random secret xi and the resulting private key for the group is x =Σxi and the corresponding public key is Y = xG for some randomly picked generator G of G1. The DKG runs as follows.

Step i. A generator G ϵ G1 is randomly chosen by one player or by all players in that network. The generators selected by all the founding members are getting summed to perform the joint computation.

Step ii. Each player Pi randomly picks a secret xi ϵ $\mathbb{Z}*q$ and computes Y_i = x_iG. P_i sets a_{i0} = x_i and chooses a random polynomial $f_i(z)$ over Zq of degree t − 1 as follows:

$$f_i(z) = a_{i0} + a_{i1}z + \ldots + a_{i(t-1)}z_{t-1}$$

Pi broadcasts A_{ik} = $a_{ik}G$ for k ϵ [0, t−1] in the MANET. Note that $Ai0 = Yi$. Pi computes the share s_{ij} = $f_i(j)$ mod q for j ϵ [1, n] and sends s_{ij} secretly to other player Pj .

Step iii. Each Pj verifies the shares he received from other players by checking for i = 1 to n:

$$S_{ij} = \sum_{k=0}^{t-1} j_k A_{ik}$$

If the checking results as fail for an index value i, then Pj broadcasts a complaint against Pi.

Step iv. If t or more players complain against a player P_i, then P_i is considered as an attacked node of fault and disqualified.Pi reveals the share s_{ij} for each complaining player Pj.If any of the revealed shares fails then the check again, Pi is disqualified. The secret shared by a disqualified player Pi is set to zero xi = 0 and Yi equal to the identity element in G1. The set of non-disqualified players is denoted by Qualified set QS.

Step v. The public key Y = Σ $_{i\epsilon QS}$ Yi and the share of secret x

for Pj is: wj = Σ $_{i\epsilon QS}$ S_{ij}

The public verification values are: Ak = $\Sigma_{i\epsilon QS}$ A_{ik} for k = 1 to t − 1. Note that A_0 = Y. Given any t user's P_{i1}, $P_{i2,}$ . . . ,P_{it} the secret x can be reconstructed as x= Σ $Lil(0)wil$ where Lil (j) =Π $_{1\le r\le t,r}$ $lj-ir/il-ir$ is the Lagrange coefficient for Pil and wil is the secret share of Pil . Note that wiG = Σ i_kAk for i ϵ [1, n].

2.5.2 Threshold Private Key Extraction

The private key for an identity ID is $xH(ID)$ where x is the server private key. When a new member with identity ID wishes to obtain his private key, he needs to obtain shares from t members selected by the IDs of the group.

The private key extraction is as follows:

Step i) the new member $Pnew$ obtains a share from P_{il} for $l \in [1, t]$: $\sigma il = w_{il}H(ID)$.

Step ii) $Pnew$ can check the validity of σil as follows:

a) Compute $wilG$ using the following formula

$$W_{il}G = \sum_{k=0}^{t-1} i_k A_{ik}$$

b) Check $\hat{e}(w_{il}G, H(ID)) \stackrel{?}{=} \hat{e}(G, \sigma_{il})$. σ_{il} is valid if the equality holds.

Step iii) To reconstruct its private key $xH(ID)$, $Pnew$ Computes

$$xH(ID) = \sum_{l=1}^{t} L_{il}(0)\sigma_{il}$$

III. Simulation Results

We compare the performance of the proposed scheme with an existing scheme, in which PKG nodes are selected randomly without consideration of the security. We further show the improvement of network lifetime and security. Obviously the performance of the network also gets increased. We also show this performance improvement through our simulation results using NS2.

3.1 Security Analysis

In our proposed scheme, PKG nodes selection is performed by IDs based on security and energy level. Nodes less than the certain energy level are not selected only node with high priority is selected, obviously the lifetime of the network, functionality and security has improved. Therefore, our scheme will have better performance than the existing scheme.

Each node has different identities, Hash function is used to map the identity of each node. DPKG protocol is used to securely generate private key , The security of the share wil of the PKG's private key x held by a founding member Pil is assured in the process of TPKE, since each σil would not leak out wil due to the difficulty to compute discrete logarithm in the group G1.The hardness of the discrete logarithm problem also ensure that a non-founding member cannot use the shares obtained from the founding members for his private key $xH(ID)$ to obtain any share of x.

The secret sharing scheme assures that at least t founding members are needed to construct the PKG secret key x or issue a valid secret key for a given identity ID.so our proposed scheme is highly secure. And they efficiently and securely perform the key generation in the distribution manner against the attacks like DoS, impersonation, malicious attacks.

3.2 Simulation Model and Parameters

We use NS2 to simulate our proposed Security enhancement in DPKG for IBC using intrusion detection (SEDPKG for IBC). In our simulation we are comparing the performance of the existing system, in which nodes are selected randomly without considering any security condition to function in the process of PKG with our model only optimal node is selected for function in the PKG process.We are evaluvating the performance according to the following metrics. In our proposed we are evaluating the performance improvement based on two parameters, with different transaction rate and varying the number of nodes for same metrics. Our simulation settings and parameters are summarized in table 1

No. of Nodes	100
Area Size	1500 X 300
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Speed	5m/s
Pause time	0,10,20,30 and 40 s
Rate	250Kb

Table 1. Simulation settings and Parameters

Drop: it is the number of packets dropped during the data transmission. Fig 1 shows the drop rate over the existing

system. In our simulation we are changing the number of nodes and Transaction rate to show this improvement. Fig 2 shows the same with different transaction rate.

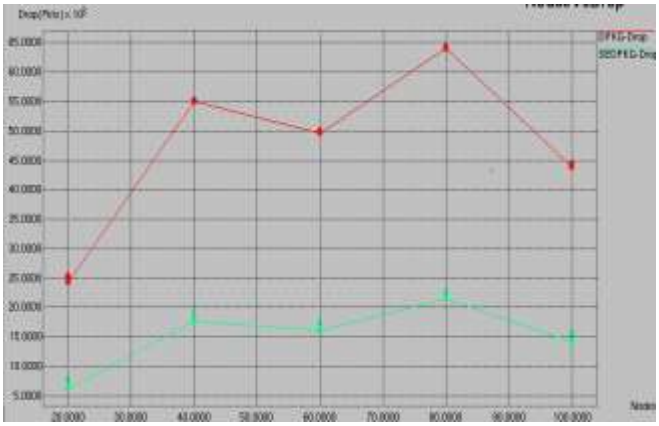

Fig. 1. Comparison of drop rate with varying the number of nodes.

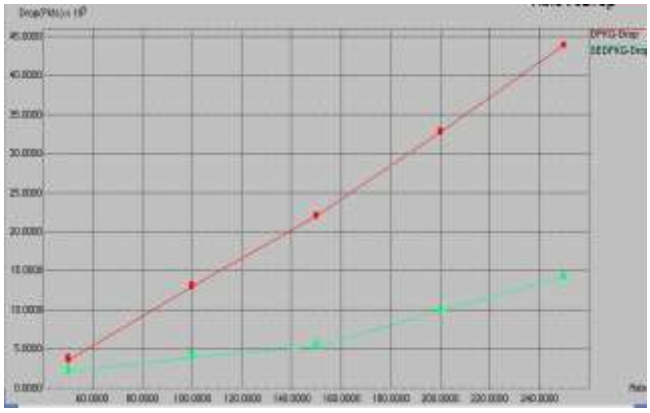

Fig. 2. Comparison of drop rate with varying the Transfer Rate.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

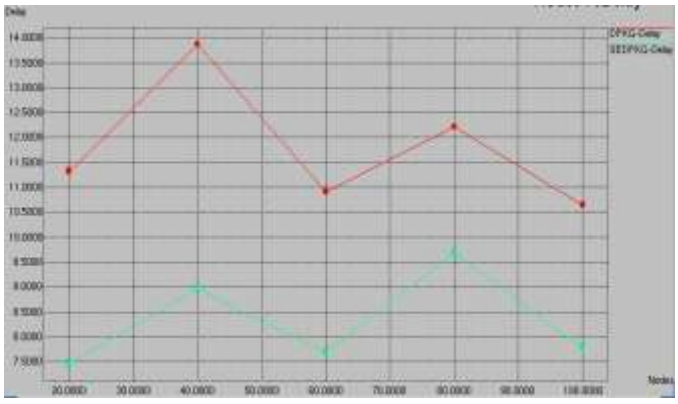

Fig. 3. Comparison of delay with varying the number of nodes

Fig 3 shows the average delay over the existing system using varying the number of nodes. Fig 4 shows the same with different transaction rate.

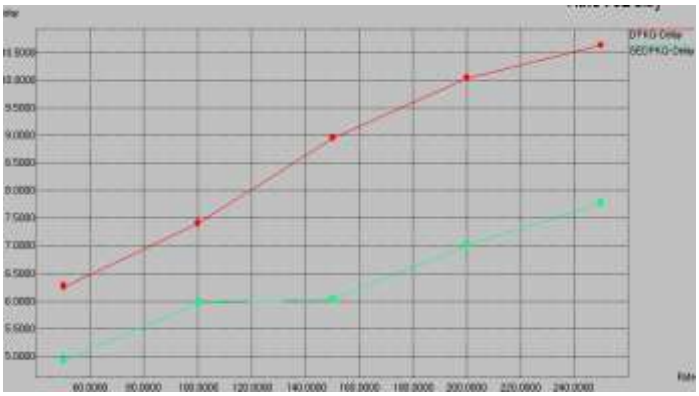

Fig 4. Comparison of delay with varying the Transfer Rate

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total no. of packets sent. Fig 5 shows the average packet delivery ratio over the existing system using varying the number of nodes. Fig 6 shows the same with different transaction rate.

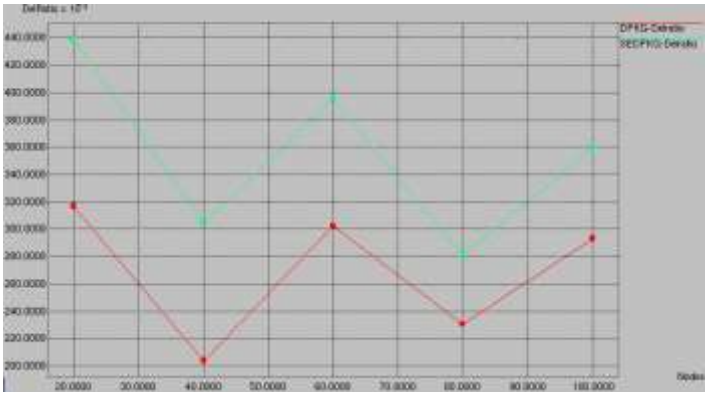

Fig. 5. Comparison of delivery ratio with varying the number of nodes

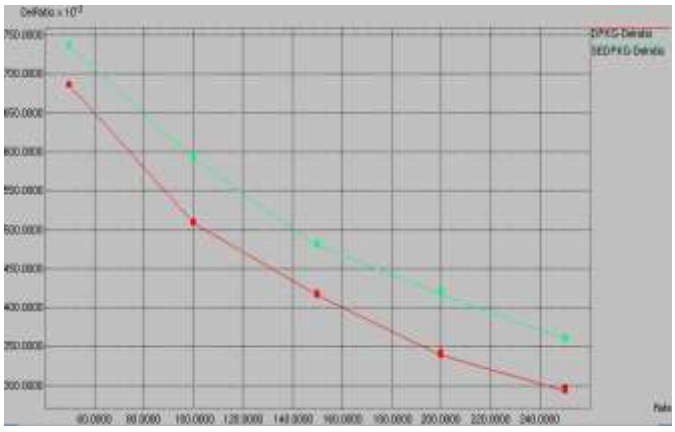

Fig. 6. Comparison of delivery ratio with varying the Transfer Rate

Energy consumption: It is the amount of energy consumed by the nodes for the data transmission.

Fig 7 and Fig 8 shows the performance improvement over the existing system.

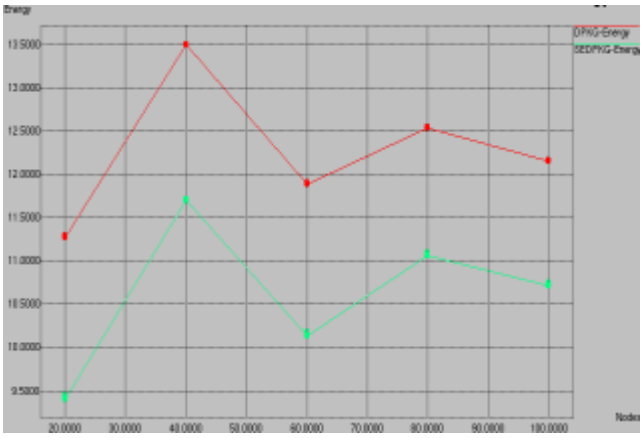

Fig. 7. Comparison of Energy consumption with varying the number of nodes

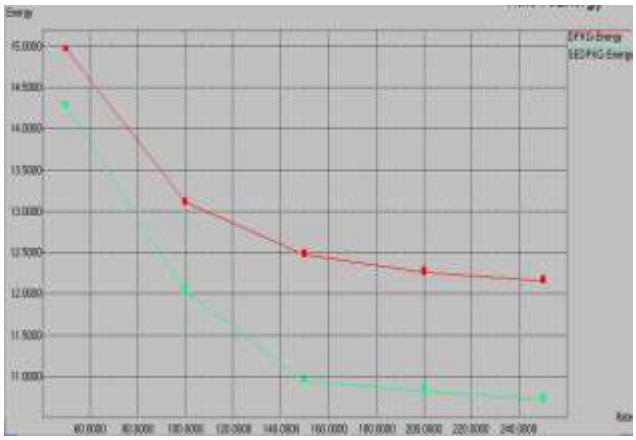

Fig. 8. Comparison of Energy consumption with varying the Transfer Rate

Overhead: it is the number of error packets included in the transaction. Fig 9 and Fig 10 shows the overhead over the existing system by varying the number of nodes and different transaction rate.

Fig. 9. Comparison of overhead with varying the number of nodes.

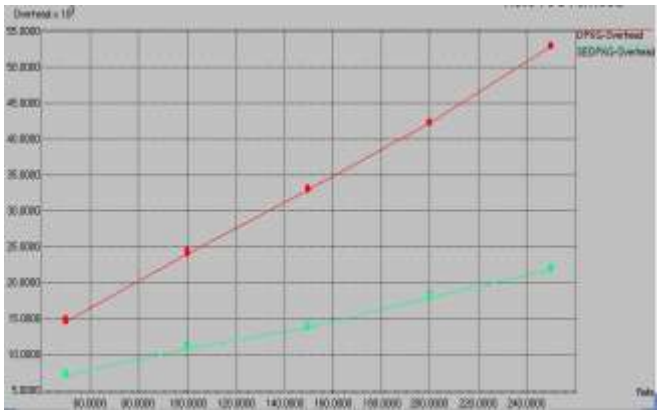

Fig. 10. Comparison of overhead rate with varying the Transfer Rate.

3.3 Network lifetime improvement

In our model we are selecting only the best node based on the energy and security condition nodes with high energy level only selected obviously the network life time is improved. We are selecting the threshold the node with certain energy level only allowed in the Key generation process low energy nodes are avoided. Thus the network life time is increased. When the number of nodes in the network is increased the network life time also increased.

IV. DISCUSSIONS

When a user wants to communicate with others or if it wants to join in the group it want to construct its private key by itself, thus the self organizing nature is preserved. For that it wants to know about the secret given by PKGs in the form of t shares. Each node has different identities, identities are unique ID hash function is used to map the identities. Due to the difficulties in the discrete logarithm

problem any new coming member cannot use the shares generated by the PKG nodes to construct its private key. The legitimate of the new coming member is ensured by obtaining t shares from the founding members. Here the selected PKGs are responsible for generation of secret, suppose selecting the node as PKG, that is already under attack or a compromised node it may send the bogus information to become as an authorized user it will possess the security vulnerability in the ad hoc network. Due to the distributed nature of the ad hoc network the state of the node may change dynamically. So in our proposed system we are implementing the same DPKG protocol but the PKG nodes are selected based on two constrains, the constrains we used in our proposed are the security and the energy level. Also in our proposed the selection of this PKG nodes are performed by intrusion detection nodes. This intrusion detection nodes are distributed in the nature it monitor the nodes energy level and security state periodically based on the received information an table is constructed by this Ids in which the nodes are ranked in the ascending order based on security state and energy level. So the Ids select the optimal node to function in the PKG process. The nodes having the lower energy levels are not selected obviously the compromised nodes energy level is become very less. In our proposed method the security is get enhanced, network lifetime and functionality is improved. Performance of the proposed scheme is increased.

V CONCLUSION

In our paper, we have presented a new key generation scheme DPKG for IBC using intrusion detection systems, which we believe would be well suited for secure key generation in ad hoc network. In our model we are dynamically selecting the optimal node for function in the PKG process using intrusion detection system. IDs act as a filter for the malicious attack as well as selecting the best node based on the security and energy constrains. In the DPKG protocol implementation the legitimate of the new coming member is authorized by t founding members that are selected in very secure manner using IDs thus in our proposed system the security is enhanced. Our simulation results show the significant improvement in security, performance and maximize the network life time.

REFERENCES

[1] Chan, *A.C.-F.* Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks, IEEE wireless communications letters, vol. 1, no. 1, February 2012.

[2] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings IEEE Symposium on Foundations on Computer Science (FOCS'87).

[3] A. Kate and I. Goldberg. Distributed private-key generators for identitybased cryptography. In SCN 2010, pages 436–453, 210.

[4] Fei Wang , Helen Tang , Peter C. Mason ,and F. Richard Yu, A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks, IEEE transactions on network and service management, vol. 7, no. 4, december 2010

[5] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos**,** Detecting Critical Nodes for MANET Intrusion Detection Systems, National Institute of Standards and Technology

[6] Farzaneh Pakzad (Corresponding author) Tiran Branch, Islamic Azad University, Tiran, Iran, Intrusion Detection Techniques for Detecting Misbehaving Nodes, Vol. 4, No. 1; January 2011

[7] Vinay P.Virada, Intrusion Detection System (IDS) for Secure MANETs: A Study, International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 6

[8] Yuvraj Singh* and Sanjay Kumar Jena, Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad hoc Networks, International Conference on Parallel, Distributed Computing technologies and Applications (PDCTA-2011)

[9] John A. Clark, Sevil Şen, intrusion detection in mobile ad hoc networks, Department of Computer Science, University of York, York, UK, YO10 5dd