Random Key Pre-Distribution Scheme: A Security Based Protocol for MANETS

Anju M A
M. Tech Scholar
Department of Electronics & Communication Engineering
M.E.A Engineering College Kerala, India

Febina P
Assistant Professor
Department of Electronics & Communication Engineering
M.E.A Engineering College Kerala, India

Abstract

Totally self-organized, self-operated, resource constrained nodes of MANETs (Mobile Ad-hoc Networks) require unique, distinct and persistent identity per node in order for their security protocols to be viable. MANET is a wireless multihop network formed by a set of mobile nodes which do not rely on an established infrastructure. The network relies on the collaboration of nodes to forward the packet to each other. While building MANETS for civilian applications some nodes tend to be disruptive or manage to save their resources through selfish behaviour. Thus the significantly degrade the performance. To cope with this, nodes of such behaviour have to detect and isolate. Random Key Pre-distribution (RKP) scheme has used to avoid the effect of selfish and malicious nodes in the network. RKP is a cryptographic approach to reduce the detection time, reduce the overhead and increase the precision of detection and improve the performance of the system.

Keywords: MANET, RKP, cryptographic approach, selfish nodes, malicious nodes

I. INTRODUCTION

MANET [1] is the new emerging technology and the most prevalent areas of research in recent years. Regardless of the geographical location it enables nodes to transfer information without centralized administration and without relying on any established infrastructure. The MANET consist of wireless mobile nodes that dynamically and freely self organizes into arbitrary and temporary ad-hoc network topologies. They allow extreme network flexibility by their properties of self-forming, self-maintaining and self-healing. Data forwarding is done in cooperation of mobile nodes within the communication range. The nodes of MANET are low cost. So they are not tamper resistant, have limited memory, limited bandwidth and often low transmission reliability. The network lifetime will be very high compared to battery life, Impracticability of using public key cryptosystems. These characteristics cause misbehaviour in nodes; 1) Selfish behaviour [7, 1, 2]: The nodes deny to forward the data packets to maximise their own gain without regard to the welfare of other nodes, 2) Malicious behaviour: That causes harmful effects on the network by providing misroute, corrupt or drop packets, 3) Lazy nodes or inactive nodes are predominantly inactive in forwarding packets to others. Paper focus on selfish nodes and malicious nodes in MANET.

For the establishment of secure communication infrastructure for a network, it requires a protocol. The design of this protocol is an important challenge. Before deployment the nodes will be pre-initialized with some secret keys [9, 16] which is the secret information. The nodes are unknown to each neighbour node. This protocol should help the network not only to enable secure communication, but also should help to allow nodes deployed at a later time to join the network securely. There are numerous limitations for MANETS.

Random Key Pre-Distribution Scheme (RKP) [2] mechanism has implemented here. RKP is a cryptographic approach [11]. Brief description of its operation has given. From key space, random pool of keys has selected. Before deployment of nodes in its service area each sensor node receives a random subset of keys from the key pool. If two nodes find a common key in their subset, they can initiate communication. Vulnerable nodes have removed by revocation method. Node to node authentication and digital signature are provided for transmitting messages.

The sections are organized as follows. Section II explains the Network architecture of the MANET. Section III explains limitations of the MANET. Section IV contains necessary conditions to be satisfied by bootstrapping scheme. Section V contains Evaluation metrics which describes the characteristics of key setup to avoid vulnerability. Section VI describes existing approach CoCoWa. Section VII describes Key Pre-Distribution Scheme. In Section VII we evaluate and analyses its working and in Section IX we compare with other approaches. In Section X we conclude the project and in Section XI we detail the future scope.

II. NETWORK ARCHITECTURE

MANETs contains several sensor nodes. Sensor nodes are low cost, highly power constrained, limited in computation and information storage capacity, communicates over only a short range wireless network interface. The network implemented with a RKP scheme. This project can be used for civilian applications as well as for military applications. Here the communication is only between neighboring nodes.

Berkeley Mica Motes [3] are an example of a sensor node's hardware configuration. 8 bit 4MHz Atmel ATmega 128L processor with 128K bytes program store and 4k bytes SRAM are its features. A minimal RISC- like instruction set is only supported by the processor. The ISM band radio receiver communicates at a peak rate of 40 Kbytes at a range of up to 100 feet. Here in real time applications this network supports up to 1000 nodes

III. LIMITATIONS OF MANETS

The high challenge in the design of security protocols and bootstrapping problem is made by these characteristics of MANETs [13].

1) Public key cryptosystems are impractical. The undesirable properties for this condition are limited power resources and computation of the sensor nodes. So RSA signature and Diffie Hellmann Key agreement cannot be used. This causes denial of service attacks.
2) Vulnerability of nodes The sensor nodes are low cost and tamper resistant. So there are chances of physical attacks. Some adversaries may take control of the node and compromise the key.
3) Architecture of post deployment configuration is unknown Here through random scattering the nodes are established. So before deployment the nodes who are neighbours cannot be found.
4) Memory resources are limited The storage capacity has a limit. So unique keys can't be established with all neighbouring nodes in the network.
5) Limited bandwidth and transmission power Has low bandwidth and the transmission of huge blocks of data are expensive.

IV. THE NECESSARY CONDITION TO BE SATISFIED BY BOOTSTRAPPING SCHEME

1) Secure node to node communication should be established by deploying nodes.
2) The additional nodes deployed at a later time should establish secure communication with the existing network.
3) Vulnerable nodes should not establish communication with the network.
4) The scheme is not aware about which node will be the neighbours.
5) The storage and computational requirement must be low.
6) The scheme should be robust to Denial of Service attack.

V. EVALUATION METRICS

The desirable characteristics in a key setup scheme which avoid vulnerability

1) Communication overhead: -
   The node must broadcast a little information as potential for key establishment.
2) Memory: -
   Reduce the number of keys as possible.
3) Scalability: -
   When demand comes up the system must be able to add more nodes.
4) Computation overhead: -
   The scheme should have low numbers of calculations for key establishment.
5) Key connectivity: -
   The communication between neighbouring nodes should be higher when the probability that the nodes share a common key.
6) Resilience against node capture: -
   Here checks by a capture of 'b' nodes the fraction of total network communications that have compromised which are indirectly linked with compromised nodes.
7) Resistance against node replication: -
   Here to check after obtaining some secret information to an adversary then whether the adversary can insert additional hostile nodes into the network.
8) Revocation: -
   Here to check whether a detected misbehaving node can be removed dynamically from the system.

VI. COCOWA

Collaborative Contact Based Watchdog (CoCoWa) [4] scheme for detecting selfish nodes is used. The method combines local watchdog and diffusion module detections on the network. When the local watchdog [4, 6] of a node detects the selfish node, then it can transmit the information to other nodes through diffusion modules when a contact occurs. When a selfish node is detected using watchdog, it is marked as positive and when a non-selfish node is detected it is marked as negative. When local watchdog detects a selfish node is not selfish, it is termed as false negative and when local watchdog detects a cooperative node as selfish, it is termed as a false positive. This information will be updated in the information update module. The local watchdog

has two functions. One is the detection of selfish nodes [17] and another is the detection of new contacts. The diffusion module has two functions. One is the transmission as well as the reception of positive and negative detections. A negative diffusion factor γ, the ratio of negative detections that are transmitted to neutralise the effect of false positives and negatives. Updating the information is the function of the Information Update Module. The updates are based on reputation value ρ using the based on equation (1) [2].

$$\rho = \rho + \Delta \quad \Delta = \begin{cases} +\delta(\text{PosEvt, Local}) \\ +1\ (\text{PosEvt, Indirect}) \\ -\delta(\text{NegEvt, Local}) \\ -1\ (\text{NegEvt, Indirect}) \end{cases} \quad \delta \geq 1 \qquad (1)$$

where δ is the increment or decrement provided for reputation value for the local watchdog detection and θ is the threshold. Here the detection time is found and also the overhead of transmission. Here the watchdog reduces the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, and malicious nodes. Here better solution for the probability of malicious nodes greater than 0.2 is obtained when δ =θ= 2 and δ=θ= 3, where δ is the increment or decrement provided for reputation value for the local watchdog detection and θ is the threshold. The detection time is reduced ranging from 20 percent for very low degree of collaboration to 99 percent for higher degree of collaboration. The harmful effects of false positives can be removed by selecting an appropriate negative diffusion factor.

VII. KEY PRE-DISTRIBUTION SCHEMES

Key PRE-distribution schemes [2, 3] can be classified broadly into probabilistic, deterministic and hybrid solutions.

1) Probabilistic: From the key pool, the key rings are randomly taken out and located in sensor nodes. With a certain probability to nodes communicate with each other.
2) Deterministic: Following some definite form key chains are placed on sensor nodes.
3) Hybrid: The two above approaches are combined here.

A. Random Key Pre-Distribution Scheme

The proposed RKP scheme is a Probabilistic approach. The RKP scheme achieves strengthened security under small scale attack, increase the security of keyset up so that to eavesdrop communication between nodes the attackers have to compromise many nodes.

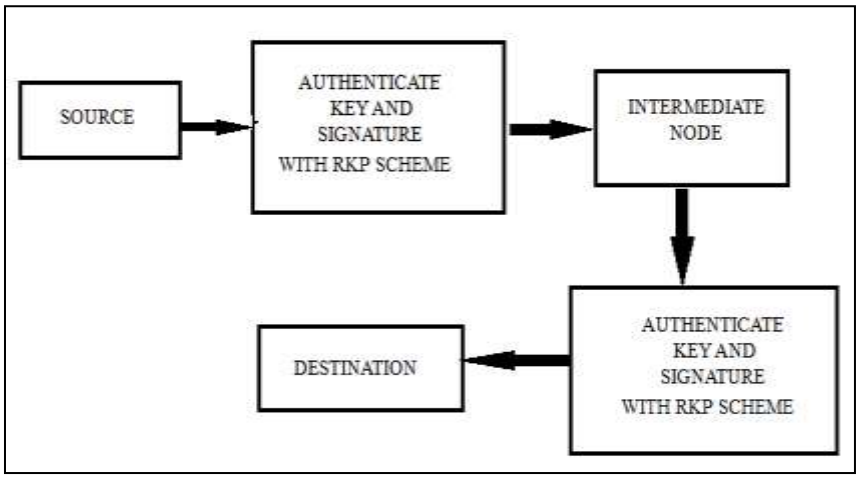

Fig. 1: Block Diagram of the proposed method

If some nodes are compromised in a network these nodes are eliminated and make the network fully secure. This scheme enables node to node authentication, node revocation mechanism and digital signature. It is significant to discuss shared key discovery and path key establishment while discussing key pre-distribution. It is because without the two key pre-distribution is incomplete. Here the nodes share a common key between them to communicate. If there is no common key between nodes, then a path key has to establish. Nodes have limited storage, so limited no of keys can only be stored in the network.

Here the network robustness against node capture attack is shown by resilience. In these attacks node captures leads to the revelation of the node's key set and the node link which use this common key will get jeopardized. Resilience fail is a function of number of compromised nodes and it is defined to be the probability that communication between two non-compromised nodes could be eavesdropped when nodes are compromised at random. Scalability characterizes the ability of a scheme to grow. When network size grows the operation of the network does not degrade. Network extension and re-deployment has to be supported by providing enough key rings by this key pre-distribution scheme.

1) Initialization phase

From the total key space a random set of keys 'R' is selected. Each node stores distinct '*x*' key forms a subset of 'R'. The '*x*' distinct keys are selected from 'R'. This '*x*' keys form the 'key ring' of the node. The probability that each subset share a common key is '*l*'. The sensor nodes are deployed. Before deployment sensor nodes do not have the knowledge of its neighbour node. The number of nodes that the network can have is:

$$x = nl \qquad (2)$$

B. Key setup phase

Key discovery phase utilise client puzzle method which is secure, but a little slower. Each node issue *x* puzzles to neighbouring node and the node which responds with correct answer have its associated key '*e*' and thus that node's identity is known. Each node holding the key '*e*' also holds the identity of the other node holding '*e*'. Now node authentication happens and a secure link is created. We compute $|R|$ as follows. Let *l(f)* be the probability that any two nodes have exactly '*f*' keys in common. Any given node has $\binom{|R|}{f}$ different ways of picking its '*f*' keys from the key pool of size $|R|$. Then total number of ways for both nodes to pick '*f*' keys each is $\binom{|R|}{f}^2$. After the '*f*' common keys have been picked, there are *2(x-f)* distinct keys in the two key rings that have to be picked from the remaining pool of $|R|$-*f* keys. Then we have

$$l(f) = \frac{\binom{R}{f}\binom{R-f}{2(x-f)}\binom{2(x-f)}{x-f}}{\binom{R}{x}^2} \qquad (3)$$

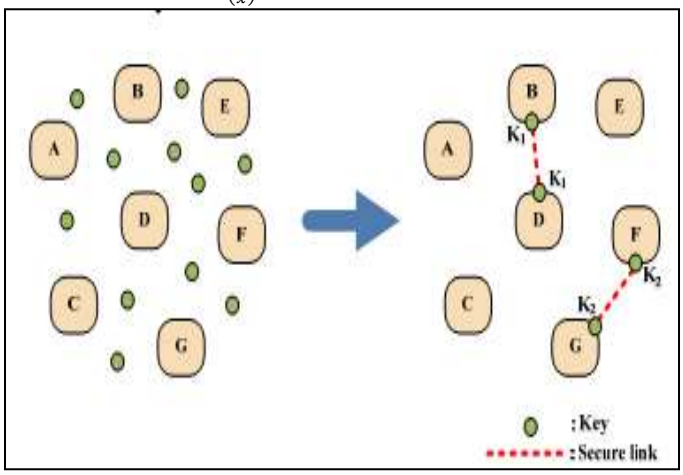

Fig. 2: Secure link establishment

In the node's vicinity to nodes to which they do not share a common key from their key ring path keys are set up. Path keys are generated using the extra keys in the key ring other than common key. Then a connected graph is formed. Now a node can generate a path key and it send securely via the path to the target node. Since the common key shared between nodes is residing in other nodes, if that node is compromised the security of the link between those nodes sharing the common key is jeopardized. We will update the key after a period to avoid such situations. This will do through multiple independent paths. At first cluster [8] the neighbouring nodes. To minimize the battery energy in the network, clustering technique is a good routing solution. Cluster head forms a cluster and the information of surrounding environment are collected by cluster member and send it to cluster head. To prevent the transmission of redundant or similar information which causes flooding of inefficient query the cluster head performs a data combination. During link disconnection and node movement, the cluster head of each cluster cannot act as a head. At that instant, the information of member node cannot be sent to the head node. The cluster head node and its member node must have a shared key to communicate in the cluster. So after forming clusters, the two hop neighbours and disjoint paths can be easily established. There are '*g*' disjoint multiple paths with two hops between the nodes that share common key. Then a node generates '*g*' random values of the same length and transmits it through *g* disjoint paths, then when it reaches the target node new link key is generated such that:

$$e' = e \oplus l1 \oplus l2 \oplus \ldots\ldots\ldots l\text{g} \qquad (4)$$

only if all the '*g*' disjoint paths are compromised the adversary can eavesdrop the communication.

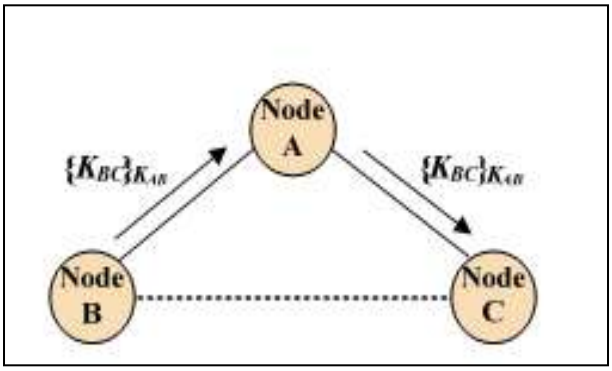

Figure3: Path Key establishment

C. *Key Revocation Phase*

Distributed node revocation scheme [2,3] is implemented in this paper. Here watchdog in each sensor node detects the misbehaviour such as selfishness of a node.

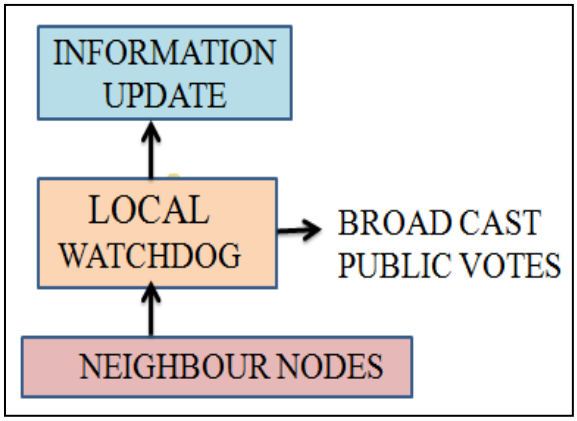

Fig. 4: Detection of selfish nodes

Then the neighbouring nodes broadcast public vote against the misbehaving node. If a node observes more than a threshold '*h*' number of public votes against the misbehaving node, it completely cuts off all the communication with that node.

Here some adversary tries to attack in this phase. This can be avoided by distributing the deactivated form of revocation key to the voting members of a particular node. The revocation key 'e_{2f}' of node 2 will be stored by *f* voting members masked with some secret x_{2f}. Only node 2 knows the activation secret. So during the key discovery and set up phase, node 2 transmits the activation secret for its voting members. The voting members verify whether it's the valid revocation key. The degree (number of neighboring nodes) of a node is limited. So if a malicious node tries to make a connection with other node searching the degree of a node in its memory the fake attempt can neglect. So the malicious nodes and selfish nodes can be removed from the network.

D. *Communication Phase*

Now the data transmission occurs through the secure link and path link. The node authentication has already completed. The data to be transmitted are digitally signed by nodes public key and has transmitted from source node to target node.

VIII. SIMULATION ENVIRONMENT

Here the simulator used in Network Simulator 2 [5]. The system has 40 nodes and has implemented in a wireless channel with two ray ground propagation. Mac used is 802-11. The dimension of topography is 1000 * 1000. The data rate is 2Mb and 11 Mb. The simulation time is 40 seconds. Here constant bit rate traffic has provided. Maximum packet in Queue is 10^{12} . The network has implemented in drop tail and Priority Queues. The packet rate is 512 Kb and packet size is 1000 s. The network contains 4 malicious nodes and three selfish nodes. Traffic model is CBR

A. SIMULATION RESULTS

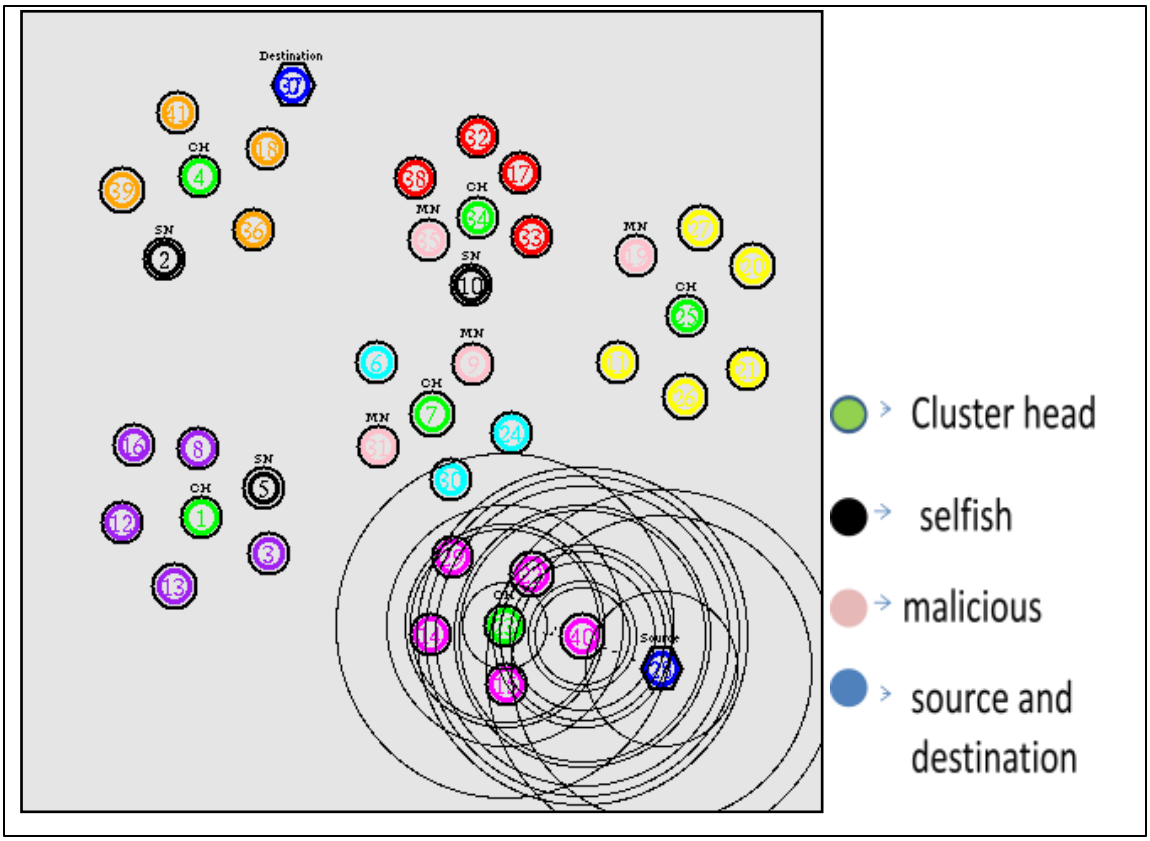

Fig. 5: GUI for RKP scheme

Output obtained while using the RKP scheme for detection of selfish nodes and malicious nodes in MANETs. It is represented in Figure 5.

B. Simulation Result using RKP scheme

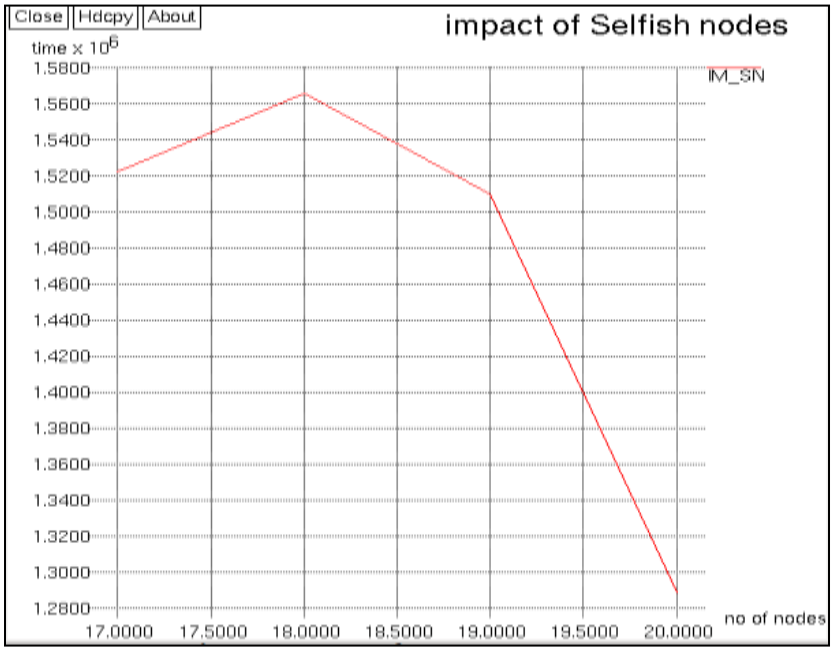

Fig. 6: Impact of Selfish nodes in MANET with RKP scheme

When using 40 nodes in network with four selfish nodes, the figure 6 shows the impact of selfish nodes. As the number of nodes in the network increases the impact of selfish nodes are reducing.

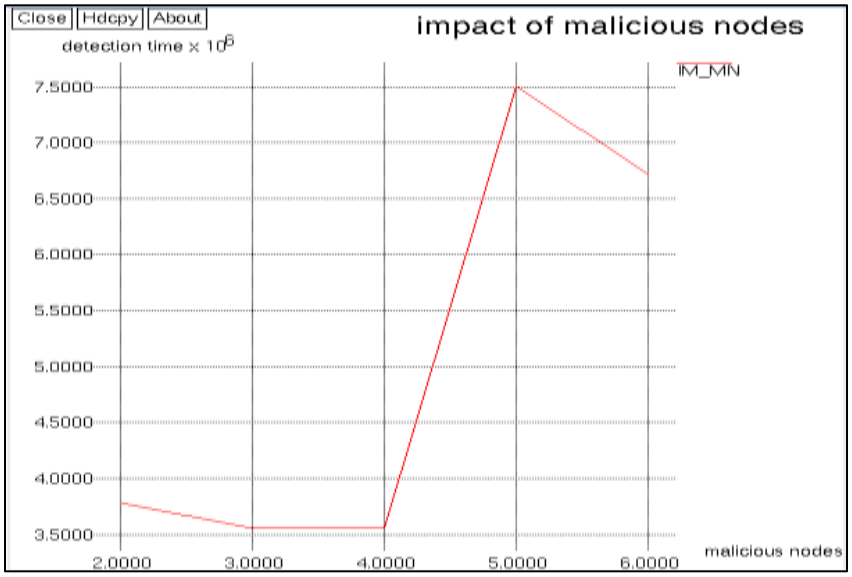

Fig. 7: Impact of malicious nodes in MANET with RKP scheme

When using 40 nodes in a network with 4 malicious nodes, the figure 7 shows the impact of malicious nodes. The detection time of selfish nodes for 4 malicious nodes in the network are very low. RKP scheme almost completely reduces the effect of malicious nodes in the network.

C. *Comparison between RKP and CoCoWa schemes*

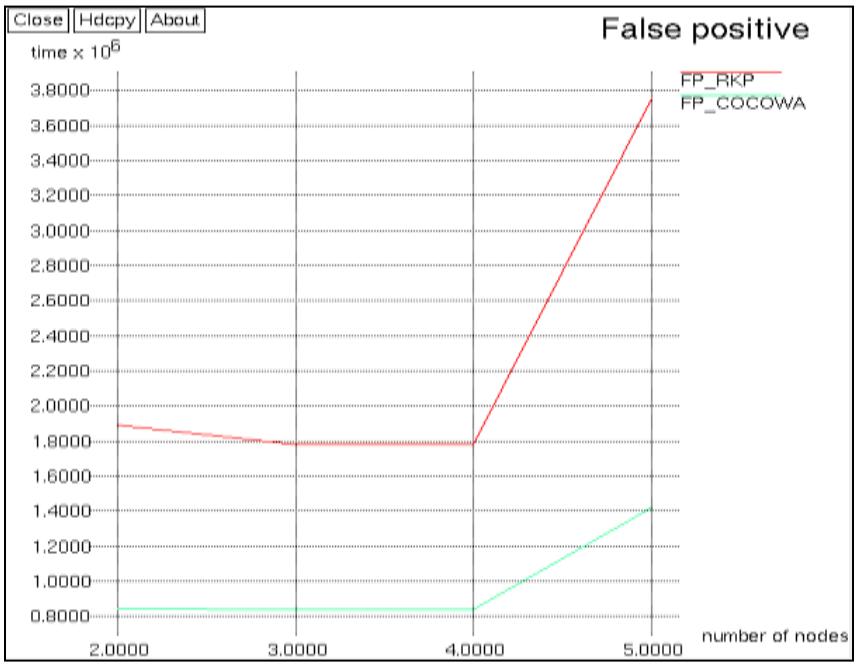

Fig. 8: Impact of False Positive while using RKP and CoCoWa

In figure 8 the impact of false positive while using RKP scheme and CoCoWa has compared. The graph is plotted between increasing number of nodes and diffusion time. Here the Red line indicated is of RKP and the green line is of CoCoWa.

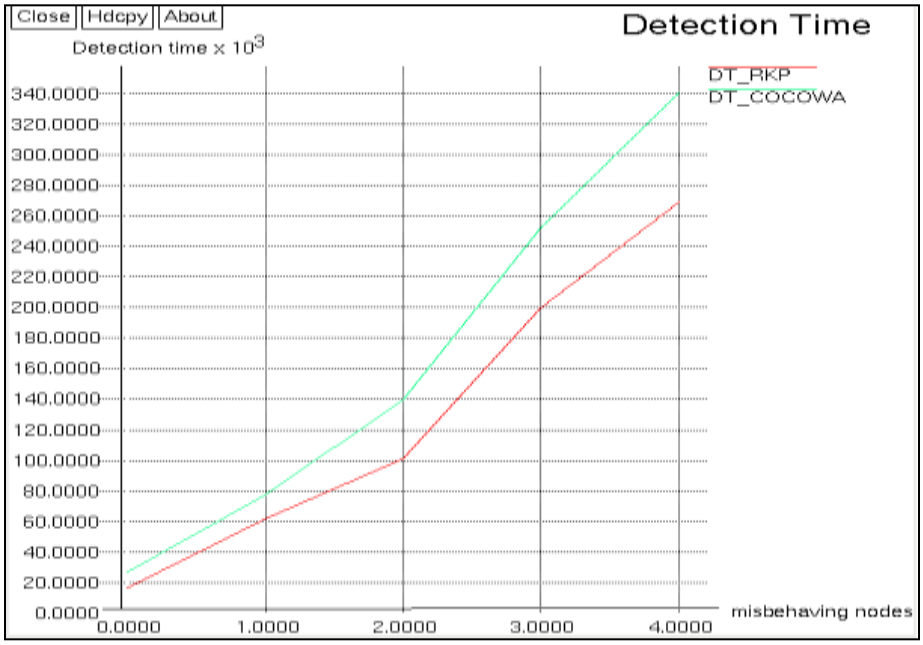

Fig. 9: Detection Time using RKP and CoCoWa

In figure 9 the detection time while using RKP scheme and CoCoWa are compared. The graph is plotted between misbehaving nodes and detection time. Here the Red line indicated is of RKP and the green line is of CoCoWa.

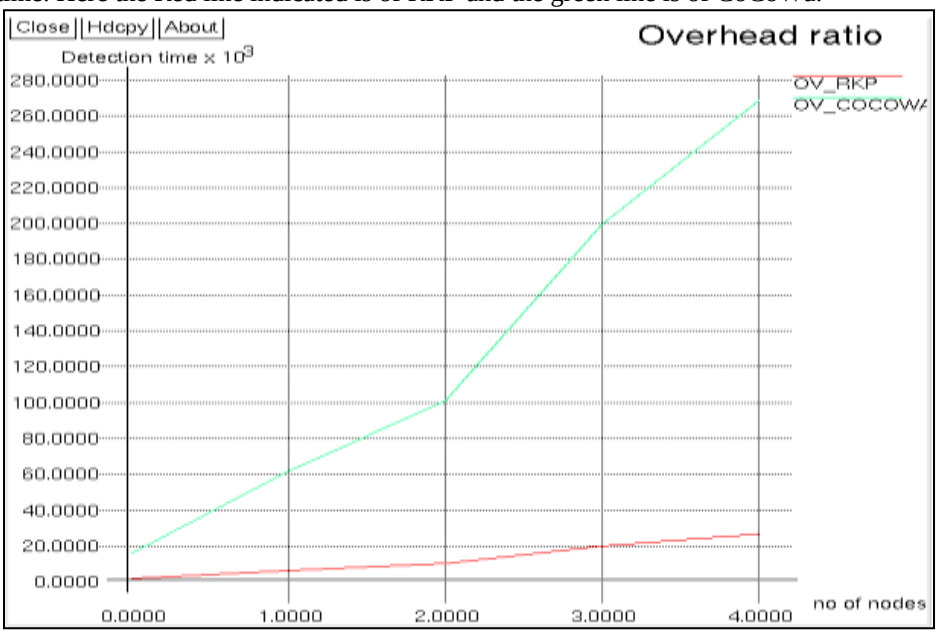

Fig. 10: Overhead Obtained for RKP and CoCoWa

In figure.10 the impact of overhead while using RKP scheme and CoCoWa are compared. The graph is plotted between the number of nodes in network and detection time. Here the Red line indicated is of RKP and the green line is of CoCoWa.

IX. COMPARISON WITH OTHER APPROACHES

The previous cooperative approaches that use periodic messages for the diffusion of selfish node detection and the CoCoWa approach are compared here. After a period P, the information about a positive detection will broadcast.

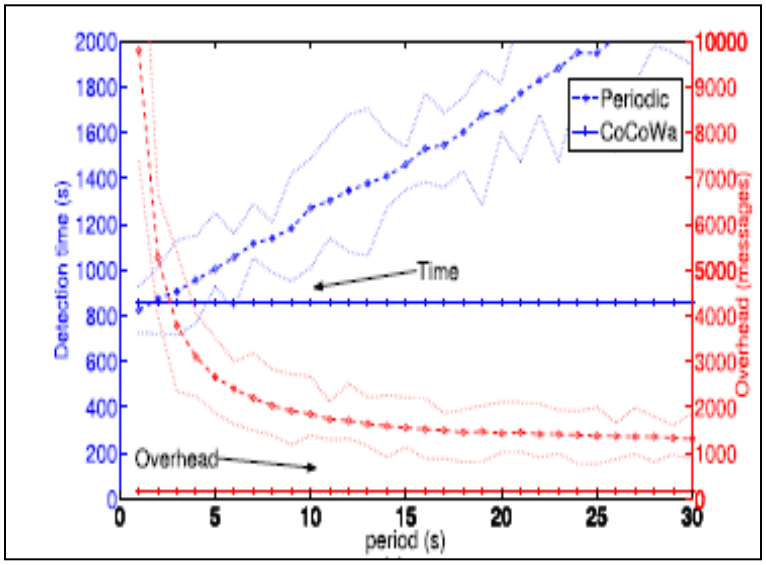

Fig. 11: Comparison of periodic diffusion and CoCoWa.[4]

D. Detection timeand overhead depending on period P for N = 40.

The nodes within the communication range of the sender will receive the message. Period P determines the performance of the protocol. The detective time is short but the overhead is high. The output of a network having a periodic diffusion protocol with 40 nodes and period P is shown in figure 11. The graph shows the detection time and overhead. The period ranges from 1 to 30 seconds. The outcome shows that by increasing period P the detection time becomes higher with reduced overhead.

Figure 12 shows the ratio between detection time and overhead [4]. Here three different numbers of nodes (N=30, 40, 50) are used. In periodic diffusion, the detection time increases compared to CoCoWa. The detection time is lower or equal to CoCoWa only in the case of reduced periods (P < 4), but the overhead is still six times greater than CoCoWa.

From the analysis, it can be summarized that although using periodic diffusion can reduce the detection time slightly, but there is a large overhead and the impact of false positives is very high, and so it is not a viable strategy for low period values.

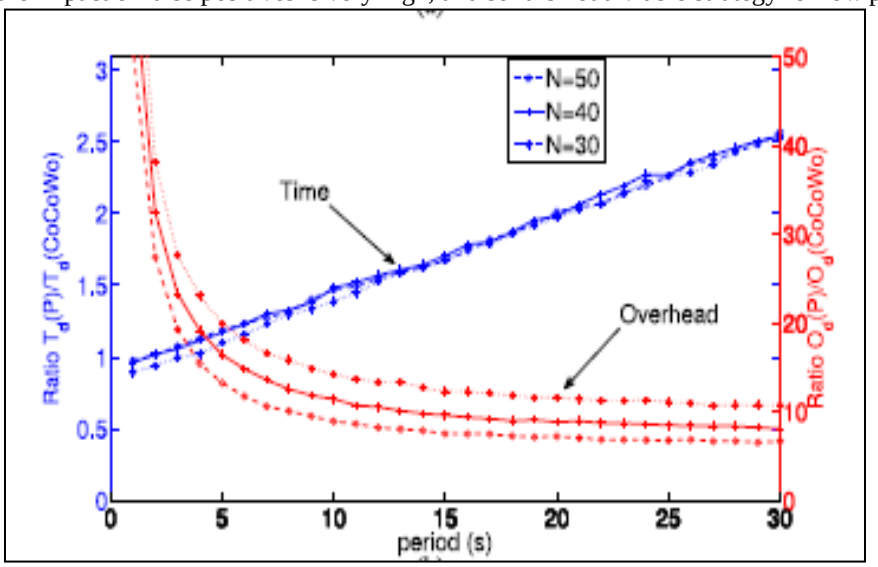

Fig. 12: Comparison of periodic diffusion and CoCoWa with increasing no. of nodes. Plot of the ratio between the detection time of periodic diffusion and CoCoWa and overhead [4]

X. CONCLUSION

The selfish nodes and malicious nodes identification and isolation are accomplished using Random Key Pre-Distribution Scheme. Three phases in this method are initialization phase, Key setup phase, Revocation phase. In Initialization phase, a set of key's called key ring established in node with one key as a common key with a probability P in the network. In the Key setup phase the common keys are found among nodes and a secure path is established. In the same phase path link are also established. Then in the revocation phase the selfish nodes and malicious nodes in the network are found and eliminated. From the simulation results, it is evident that when compared with conventional methods the proposed method has reduced the detection time,

increased precision and has less overhead when detecting selfish and malicious nodes and the effect of false positives has reduced. Reduction of overhead messages ranges from 10 percent for very low degree to 100 percent for higher degrees of collaboration. RKP scheme has reduced the effect of malicious nodes, false positives and selfish nodes quickly.This security protocol can be used in civilian networks as well as military networks.

XI. FUTURE SCOPE

As there are many applications of MANET both in civilian environment and military environment it is important to keep the security of system. The selfish nodes and malicious nodes are commonly seen in MANET. As these nodes degrade the performance of system these nodes have to detect accurately with in short time and with less overhead. So other efficient and superior methods can be generated.

REFERENCES

[1] E. Hernandez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.
[2] H. Chan, A. Perrig, and D.Song, "Random Key pre-distribution schemes for sensor networks," IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14, 2003, pp. 197-213.
[3] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," IEEE Symposium on Research in Security and Privacy, 2003, pp. 197-213
[4] Hernandez-Orallo, E.; Serrat Olmos, M.D.; Cano, J.-C.; Calafate, C.T.; Manzoni,P. CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish NodesMobile Computing, IEEE Transactions onYear: 2015, Volume: 14, Issue: 6 , Pages:1162-1175
[5] Issariyakul, Teerawat, and Ekram Hossain. Introduction to network simulator NS2. Springer Science & Business Media, 2011.
[6] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in Proc. Int. Conf. Commun. Workshop, 2010, pp. 1–5.
[7] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.
[8] L. B. Oliveira, H. C. Wong et al., "SecLEACH - A random key distribution solution for securing clustered sensor networks," in Proc. Fifth IEEE International Symposium on Network Computing and Applications, 2006, pp. 145-154.
[9] L. Eschenauer and V. Gligor, "A key management scheme fordistributed sensor networks," in Proc. the 9th ACM Conf. On Computer and Communications Security, NewYork: ACM Press, pp. 41-47, 2002.
[10] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, "On the effect of node misbehavior in ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2004, pp. 3759–3763.
[11] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks,"IEEE Trans. Mobile Comput.,vol.10, no. 7, pp. 997–1010, Jul. 2011.
[12] Priyanka Goyal, VintiParmar and Rahul Rishi, "MANET: Vulnerabilities,
Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
[13] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.
[14] S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 19–33, Jan. 2008.
[15] S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997.
[16] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proc. The Tenth ACM Conference on Computer and Communications Security (CCS 2003), 2003, pp. 42-51.
[17] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," IEEE Trans. Veh. Technol., vol. 60, no. 5, pp. 2224–2238, Jun. 2011.
[18] Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009.