International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 11 (November '2017)

A TRUST BASED SECURITY IN MOBILE AD HOC NETWORKS

G.Jeeva,
M.Phil Research Scholar,
P.G & Research Department of Computer Science,
Siri PSG Arts and Science College for Women,
Sankari,Tamilnadu,India.

K.Sumathi,
Assistant Professor,
P.G & Research Department of Computer Science,
Siri PSG Arts and Science College for Women,
Sankari,Tamilnadu,India.

Abstract: Wireless ad hoc network is a collection of mobile nodes dynamically forming a temporary network without a centralized administration. This kind of network has been applied for both civilian and military purposes. However, security in wireless ad hoc networks is hard to achieve due to the vulnerability of the links, limited physical protection of the nodes, and the absence of a certification authority or centralized management point. Consequently, novel approaches are necessary to address the security problem and to cooperate with the properties of wireless ad hoc network. Similar to other distributed systems, security in wireless ad hoc networks usually relies on the use of different key management mechanisms. The compromise of the node breaks down the whole security system.

Keywords: Mobile Ad Hoc Network, Security, Attacks, Trust Management

I.INTRODUTION

In Mobile Ad Hoc Network (MANET), a collection of nodes having wireless in nature are formed as a transitory/short-lived network not having any fixed infrastructure(as shown in fig.1). In MANET all the nodes can move freely and capable to organize themselves. Each node has dual functionality as router and host where the topology maybe changing suddenly [1]. Ad hoc networking is used wherever the infrastructure is little or without any physical communication or the existing infrastructure is costly or problematic to use. It lets the devices to preserve connections to the network and also to add or remove a device/node. There are different arrangement of uses for MANETs, running from expansive scale, portable, profoundly dynamic systems, to little and static systems which are having restricted force sources. Notwithstanding the legacy applications that move from customary framework environment into the specially appointed environment, an extraordinary course of action of new administrations will be made for the new environment. It comprises Military Battlefield, Sensor Networks, Commercial Sector, Medical Service and Personal Area Network [2].

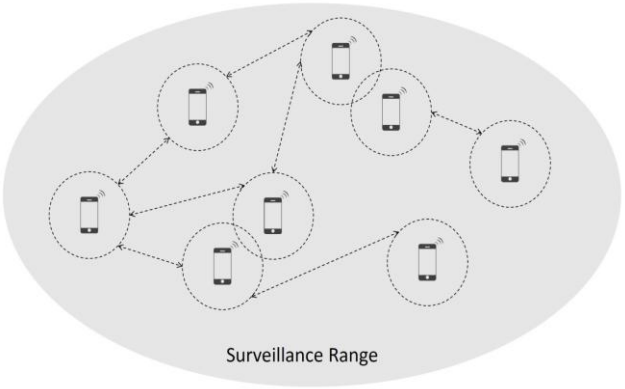

Figure 1: Ad hoc Wireless Network (MANET)

Mobile ad hoc networks are vulnerable to attacks compared to the wired networks. The wireless links between the mobile nodes are not secured for communication without imposing proper security measures. A quick and cost effective deployment is required for ad hoc wireless networks. The limited power supply causes denial-of-service attacks issue [3]. The trust relationship among nodes may be disturbed by the Dynamic topology and changeable nodes membership. If some nodes are detected as compromised, it also disturbs the trust. Distributed and adaptive security mechanism scan protect this dynamic behavior [4].

Since the self organization and maintenance properties are built into the ad hoc networks makes it defenseless against attacks. The following are the different challenges and security issues in MANET [5].

- ***Availability*:** Should withstand survivability paying little respect to DoS attacks like in physical and media access control layer assailant utilizes jamming techniques for obstruct with communication on physical channel. On network layer the attacker can intrude on the routing protocol. On higher layers, the attacker could cut down abnormal state services, e.g., key management service.
- ***Confidentiality*:** Should shield certain data which is not to be uncovered to unauthorized elements.
- ***Integrity*:** Transmitted Message ought to be honest to goodness and ought to never be adulterated.
- ***Authentication*:** Empowers a node to shield the qualities of the peer node it is imparting, without which an attacker would copy a node, in this manner

Attacks on MANETs: MANETs are inclined to a few sorts of attacks, which can essentially be ordered intotwo structures as per the way of the attacks as; Active attacks and passive attacks.

- **Active attacks** – Under such attacks, the attacker means to bring about jamming,transmitting fake routing data or interfere with nodes from giving services. A

fewcases of active attacks are Black Hole Attacks [6] and Flooding Attacks.

- **Passive attacks** – Under such attacks, the attacker tries to pick up control access over the network [7]. A passive attack does not disrupt the operation of the network, the advisory snoops the data exchanged in the network without altering it. Here the requirements of confidentiality can be violated if an advisory is also able to interpret the data gathered through snooping.

Security techniques for MANET : To preserve the security of MANETs from attacks, a routing protocol must fulfill the accompanying arrangement of prerequisites, to guarantee appropriate working of the path from source to destination in vicinity of malicious nodes,

- Authorized nodes ought to perform route computation and discovery.
- Minimal introduction of network topology
- Detection of spoofed routing messages
- Detection of created routing messages
- Detection of changed routing messages
- Avoiding development of routing loops
- Prevent redirection of routes from shortest path

II. LITERATURE REVIEW

Xiaoyong Li, *et al.* [8] LDTS facilitates trust decision making based on a light weight scheme. By closely considering the identities of nodes in clustered WSNs, this scheme reduces risk and improves system efficiency while solving the trust evaluation problem when direct evidence is insufficient. Most trust management systems proposed for WSNs adopt simple weighted average approaches to aggregate feedback trust information without considering the problem of malicious feedback. This may lead to misjudgment of the trust decision making process. But LDTS does not utilize broadcast based strategy and instead sets the value of indirect trust based on the feedback reported by the cluster head about a node. This feedback mechanism has numerous advantages such as the effective mitigation of the effective malicious feedback, thereby reducing the networking risk in an open or hostile WSN environment. Because the feedback between cluster members need not be considered this mechanism can significantly reduce network communication overhead thus improving the system resource efficiency.

Mike Burmester, *et al.* [9] as an extension to Diffie-Hellman, the group key agreement scheme is proposed by Burmester and Desmedt (B-D). Dependable multicasting is hard in wired networks, and considerably additionally challenging in ad hoc networks. Changes ingroup enrollment requires a restart of the key-agreement technique. In an ad hoc network with moving nodes, there is no probability for establishment of a group key by B-D and maintenance of later changes in-group participation. Group changes can bring about delay and interruption. B-D likewise demands an already running routing protocol or stand out hop neighbors. This implies, the key-agreement schemes rely on upon an already established routing foundation. In any case, the framework can't be established before the keys have been set up.

Klaus Becker, *et al.* [10] for reducing the complexity of existing algorithms Hypercube and Octopus (H&O), has proposed a method which minimizes the number of rounds by arranging the nodes in a hypercube. H&O contains two protocols, to be specific, Hypercube and Octopus. Hypercube expect the number of members is a force of 2. Octopus extends the Hypercube to permit a self-assertive number of nodes. H&O is helpless against MIM attacks as authentication is absent. Byzantine or defective nodes might block fruitful key agreement. Changes in group enrollment require rekeying. It is left for the nodes to choose when re-keying is required. H&O depends on a basic communication system to offer a reliable node-requesting perspective to all group individuals. H&O is unsuitable for network layer security in ad hoc networks.

N. Asokan, *et al.* [11] as an extension to the H&O, a password Authenticated mechanism is proposed which is the stand out of the contributory systems designed for ad hoc networks. It is often referred to as the H&O method stretched out with secret key authentication. This method expects that all the legal members get a secret word offline. During the pair wise D-H key agreements of the H&O protocols, the nodes must demonstrate the learning of the secret key. The secret word is utilized to encrypt the public quality and a starting test in a test reaction protocol. This scheme duplicates the number of messages and expands the computational many-sided quality when contrasted with H&O. It solves the vulnerability of H&O to MIM attacks at the cost of scalability. The scheme acquires the lacks of H&O in regards to the trustworthiness of an already established communication base and node-requesting scheme. In this manner, it is not fitting for network layer security in mobile ad hoc networks.

III. TRUSTED CERTIFICATE EXCHANGE AND REVOCATION IN MANET

The certificate exchange method offers the nodes to authenticate themselves with the individuals in the network before they some assistance with getting joined and begin another communication. With a specific end goal to improve the unwavering quality of certificate exchange protocol, Multi-path Technique is used. During the multi-path certificate exchange, the public key of a node is certified by the diverse nodes. As an aftereffect of various autonomous certifications, the certainty doled out to the certificates is higher. Also, the authentication is performed commonly. Table 1 presents the notations used in the certificate exchange technique.

When S receives k_{pud}, it issues a certificate for that public key. Consequently, D issues a certificate for k_{pus}. Each node in T(S) contains its public key certified by S since the authentication is mutual. The steps involved in the certificate exchange process are as follows.

- ***Step 01:*** S broadcasts REQ_{cert} containing ID_D and T(S) for D's certificates.

$$S \xrightarrow{REQ_{Cert} + ID_D} \text{Neighbor nodes}$$

This REQ_{cert} is sent with a minimum time to live (TTL_{min}) for minimizing the communication overhead of the protocol.

Notations	*Representation*
S	*Source Node*
D	*Destination Node*
N_i	*intermediate nodes*
kpu_d	*public key of D*
kpu_s	*public key of*
T(S)	*set of nodes certified for* kpu_s
REQ_{cert}	*certificate request message*
REP_{cert}	*certificate reply message*
C_{self}	*self-signed certificate*
ID_D	*the identity value of D*
CL	*certificate list*

Table 1: Notations used in certificate exchange technique

- ***Step 02:*** When Ni receives the REQ_{cert}, it verifies k_{pus} and checks its own CL. If, (N_i has no certificate for D) | | (N_i has already replied to the REQ_{cert}) Then, Ni forwards the REQ_{cert} to its neighbor nodes Else, Ni feedbacks REP_{cert} to S that contains the certificate of k_{pud} signed by N_i
- ***Step 03:*** If, N_i is unaware of S, Then, Ni constructs a C_{self} and notifies S that it wants to make a certificate exchange which is performed via a multiple node-disjoint paths.
- ***Step 04:*** If, N_i already has a route to D in its cache, Then, N_i informs D that S has requested its k_{pud}. D responds to query and requests a certificate for k_{pus}. Since Ni and D can authenticate each other, the communication among the D and N_i is made secured using N_i's signature. Hence there is no possibility for any node to corrupt the certificate of S which is issued by N_i.
- ***Step 05:*** If, D is unaware of adequate number of nodes Then, D replies to REQ_{cert} itself.
- ***Step 06:*** S repeats the above process by increasing the TTL value until it obtains the minimum number of certificates for k_{pud}.
- ***Step 07:*** S then calculates the trust value CT_{ij} of the nodes included in the all offered paths.
- ***Step 08:*** S considers only those paths, which are free from malicious nodes. S performs the certificate revocation process for defending against the malicious nodes.
- **Step 09:** Among the obtained paths, source selects a path which is having more certifiers of the destination node D, as explained.
- ***Step 10:*** S then forwards the first packet to D that contains the set of nodes that has offered the certificates for k_{pud}.
- ***Step 11:*** Once they have exchanged their public keys, S and D issue certificates for each other. Due to multiple independent certifications, the confidence assigned to these certificates is higher. For example, consider the Figure 2.

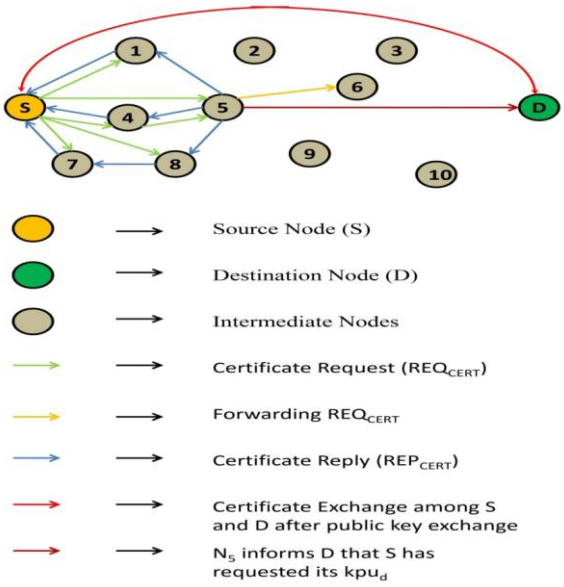

Figure 2: Certificate Exchange Technique

Demonstrate our certificate exchange mechanism by considering N5. S broadcasts the REQ_{cert} to its neighbor nodes. When N5 receives the message, it checks its CL. If N5 does not know D or it has already sent the REP_{cert}, then it just forwards it to next node N6. Otherwise, N5 replies with REP_{cert} that contains the certificate of k_{pud} signed by N5 to S. When N5 is not aware of S, then N5 constructs a C_{self} and notifies S that it wants to make a certificate exchange via multiple node-disjoint paths. i.e. through (N5-N1-S) & (N5-N4- S) & (N5-N8-N7-S). If N5 already has a route to D in its cache, then it informs D that S has requested its k_{pud} and it responds to query and requests a certificate for k_{pus}. If D is unaware of adequate number of nodes, it replies to REQ_{cert} itself. S repeats the above process by increasing the TTL value until it obtains the minimum number of certificates for k_{pud}.

IV. SIMULATION RESULTS

Simulations were performed utilizing Network Simulator (NS-2), especially well known in the ad hoc networking group. The MAC layer protocol IEEE 802.11 with a data rate of 11 Mbps is utilized as a part of all simulations. The transmission range is set to 250m. The propagation model is Two Ray Ground. The aggregate number of nodes is set to 100 nodes in 1000m x1000m network territory. In our simulation, the minimal speed is 5 m/s. The source-destination pairs are spread randomly over the network. The

ns-2 constant bit rate (CBR) traffic generator is utilized to set up the association designs with distinctive irregular seeds. Every node has one CBR traffic association with a solitary unique destination. Sources start time is consistently distributed over the initial 60 seconds of the simulation time. Change the load value as 50,100,150,200 and 250Kb. The size of certificates was likewise set to 512 bytes. The aggregate number of connections in the network was set to 20 connections. The Ad Hoc On-demand Multipath Distance Vector (AOMDV) routing protocol was decided for the simulations. The simulation results are the normal of 10 runs. The proposed system was effectively incorporated into the AOMDV protocol's route discovery mechanism. In the simulation, attacks are simulated where the attacker nodes send spurious certificates to the nodes which have requested for those certificates. These attacks can be isolated attacks where each attacker guarantees an alternate public key. In any case, the attackers might likewise dispatch an agreeable attack where a group of attackers collude and send certifications for the same public key that is spurious. Both these sorts of attacks-isolated and intrigue are simulated. Our simulation settings and parameters are summarized in table 2

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	100 to 500 sec
Routing Protocol	AOMDV
Traffic Source	CBR
Packet Size	512
Speed	5m/s
Pause time	5 seconds
Load	1000 Kb.
No. of attackers	1 to 10

Table 2 Simulation Settings for SOKMTC

Compare the proposed Self-organized Key Management for Trusted Certificate Exchange and Revocation (SOKMTC) technique with On-demand Self-Organized Public Key Management (SOPKM) scheme, Ad hoc on-demand trusted-path distance vector (AOTDV) routing protocol and Ad Hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. Select SOPKM and AOTDV among the existing works, since it is the latest work which deals self-organized key management along with certificate chains and simulated in NS-2. Evaluate mainly the performance according to the following metrics:

- **Average end-to-end Delay:** The normal time taken by the data packets from sources to destinations, including support delays during a route discovery, lining delays at interface lines, retransmission delays at MAC layer and propagation time.
- **Packet Delivery Ratio:** The portion of the data packets delivered to destination nodes to those sent by source nodes.
- **Packet Drop:** It is the number of packets dropped during the transmission.
- **Misdetection Ratio:** The proportion of the number of nodes whose conduct (malicious or generous) is not recognized accurately to the genuine number of such nodes in the network.
- **Routing packet overhead**: The number of control packets (including route request/reply/update) for establishing connection over a period of time.
- **Resilience against Node Capture:** The fraction of communications compromised to the total number of communications by a capture of x-nodes.

Varying Number of Attackers

The number of attackers is increased from 1 to 10 and the performances of the techniques are measured in terms of Delivery Ratio, Misdetection and Resilience.

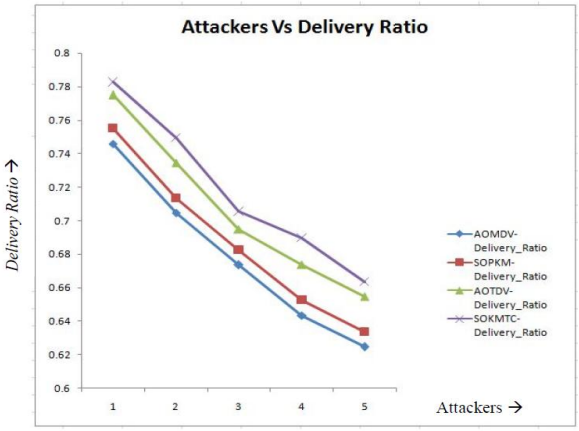

Figure 3: Packet Delivery Ratio

Figure 3 shows the average Packet delivery Ratio of the schemes, when the attackers are increased from 1 to 5. That the delivery ratio decreased linearly as the attacker increases. But, the delivery ratio of our proposed SOKMTC is greater than the existing schemes. The delivery ratio is high, because the trusted certificate exchange and revocation mechanism identifies the malicious nodes dynamically and eliminates the same immediately after the detection.

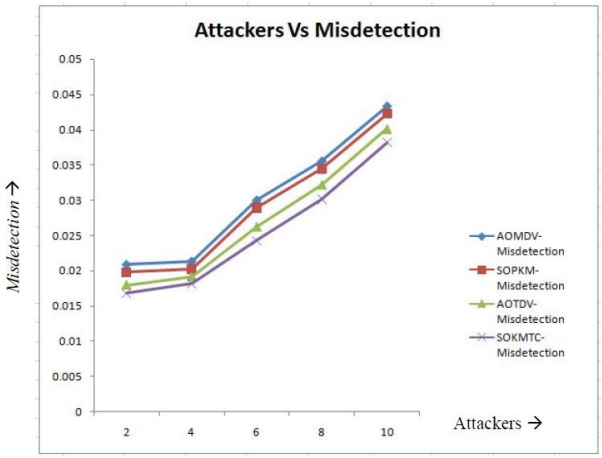

Figure 4: Misdetection Ratio

The ratio of the number of nodes whose behavior is not identified correctly to the actual number of such nodes in the network is shown in figure 4. Our proposed method is capable to detect more malicious nodes while comparing to the existing methods. The misdetection ratio is less, that means the framework can successfully detect the malicious node in time itself and able to eliminate dynamically. The result of fraction of compromised communications is shown in figure 5. Because of the trusted mechanism, the number of compromised communications is less in SOKMTC. Hence the proposed SOKMTC is more resilient than the existing mechanisms. Here the malicious nodes are identified immediately when their behavior becomes malevolent. So the ability to defend against attacks of a network is improved, that means the communications where the attacker node involved is very less.

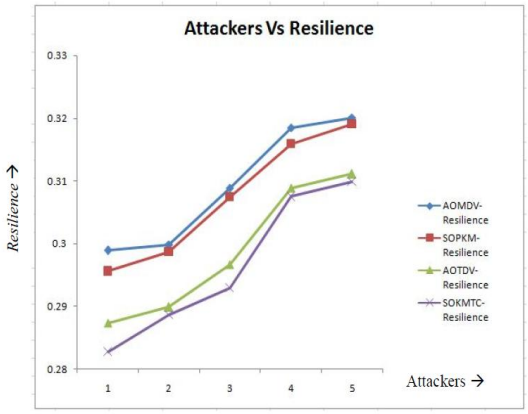

Figure 5: Resilience against Node Capture

Varying Number of Nodes : The CBR data packets and control packets dropped due to the attackers, presented in figures 6. As the number of attacker increases, more data packets are dropped. But SOKMTC has less packet drops when compared to other schemes. The dropping of packets is less for the proposed method, since the framework ensure to select the trust path, having more certifiers for communication. Figure 7 depict the delay involved in the communication by each pair of source and destinations. The number of nodes is varied from 10 to 50, and corresponding delay for the four schemes are measured. The proposed method outperforms the existing methods in case of delay. The delay is very less for the proposed method since the framework selects the trusted path, thus the path breakage problem will not affect communication.

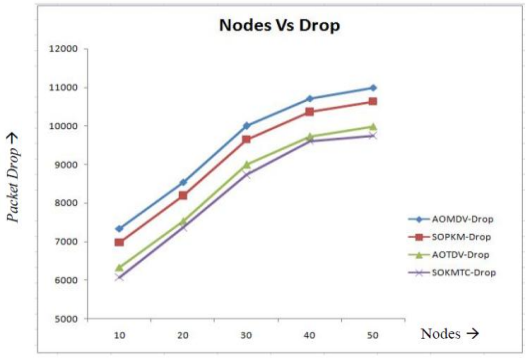

Figure 6: Packet Drop

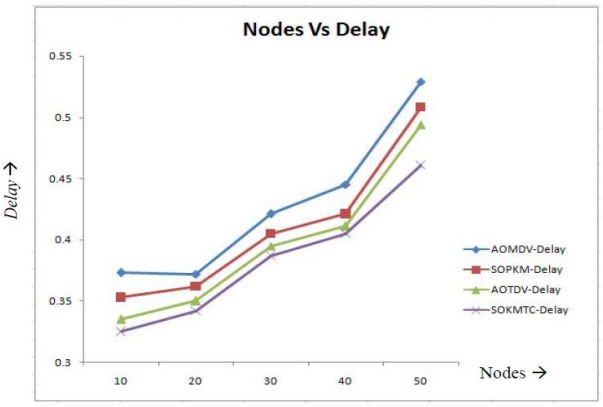

Figure 7: Average end-to-end Delay

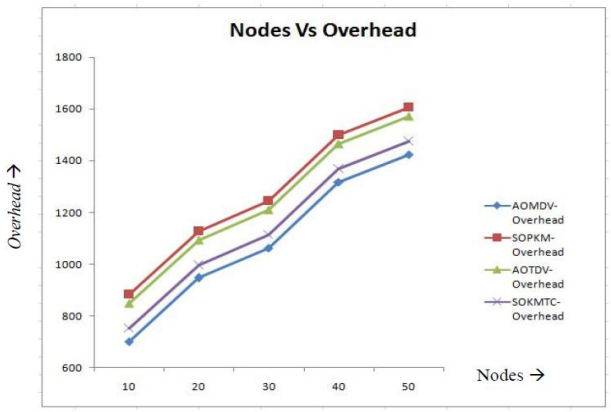

Figure 8: Routing packet overhead

Figure 8 shows the Routing packet overhead of the schemes, when the nodes are increased from 10 to 50. That the overhead of our proposed SOKMTC is greater than the basic AOMDV since the proposed method contains the trust management mechanism for certificate exchange and revocation, but it is lesser than both other schemes.

VI.CONCLUSION

The theme of the thesis is centered on one critical part of mobile adhoc networks; the trust based key management. Key management for MANET is a basic issue that has been discussed and solutions for it have been proposed in view of trust management mechanism. The key management scheme depends upon the application situation for which it is designed. A harmony between the utilization and the accessible resource of power, computation figures out which key Management mechanism is to be deployed. The trusted intermediaries are essential for keeping communications alive and free from attacks. However there is still much work to be done. The proposed trust based mechanisms in this thesis are vital for secure key management and routing in MANETS. The execution results of all the proposed techniques are exhibited utilizing differed simulation situations utilizing network-simulator 2. In this framework different aspects were discussed for establishing trust based key management in mobile adhoc networks.

VII.REFERENCES

[1]. Ke Liu, Nael Abughazaleh and Kyoung Donkang., "Location verification and trust management for resilient geographic routing," ELSEVIER, 2007.

[2]. Efthimia Aivaloglou and Stefanos Gritzalis, "Hybrid trust and reputation management for sensor networks," Springer, October 2009.
[3]. Riaz Ahmed Shaikh, Hassan Jameel, Brian J d Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," pages 1698 - 1712, IEEE Transactions on Parallel and Distributed Systems, October 2009.
[4]. Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan, and Abdul Sattar, "A trust management architecture for hierarchical wireless sensor networks," pages 268 - 271, IEEE Conference, 2010.
[5]. Idris M. Atakli, Hongbing Hu, Yu Chen, WeiShinn Ku, and Zhou Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation, " The Symposium on Simulation of Systems Security (SSSS08), Ottawa, Canada,, April 2008.
[6]. Long Ju, Hongjuan Li, Yaqiong Liu, Weilian Xue, Keqiu Li, and Zhongxian Chi," An improved intrusion detection scheme based on weighted trust evaluation for wireless sensor networks", IEEE Conference on Local Computer Networks, 2010.
[7]. Satya Keerthi, A Manogna, Yasaswini, A Aparna, and Ravi Teja, "Behaviour based trust management using geometric mean approach for wireless sensor networks," volume 3, pages 229 - 234, International Journal of Computer Trends and Technology, 2012.
[8]. Fenye Bao, Ing-Ray Chen, MoonJeong Chang and Jin Hee Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," volume 9, pages 169 - 183, IEEE transactions on network and service management, June 2012.
[9]. Xiaoyong Li, Feng Zhou, and Junping Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," volume 8, pages 924-935, IEEE Transactions on Information Forensics and Security, June 2013.
[10]. Wei Liu, Hiroki Nishiyama, Nirwan Ansari and Nei Kato "A Study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE, 2011, pp. 1-5.
[11]. Mike Burmester and Yvo Desmedt, "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, 1994, pp. 275–286.
[12]. Klaus Becker and Uta Wille, "Communication Complexity of Group Key Distribution," Proc. 5th ACM Conf. Comp. and Commun. Security, 1998, pp. 1– 6.
[13]. N. Asokan and Philip Ginzboorg, "Key Agreement in Ad Hoc Networks", Computer Commun., vol. 23, no. 17, Nov. 2000, pp. 1627-1637.
[14]. M. Steiner, G. Tsudik, and M. Waidner, "CLIQUES: A New Approach to Group Key Agreement," Proc. ICDCS'98, 1998, pp. 66-78.
[15]. Seung Yi and Robin Kravets, "MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks," Report No. UIUCDCS-R-2004- 2502, UILU-ENG-2004- 1805, University of Illinois at Urbana- Champaign, 2002, pp. 1-19.
[16]. Bing Wua, Jie Wua, Eduardo B. Fernandeza, Mohammad Ilyasa, Spyros Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IPDPS'05, 2005, pp. 52-69.
[17]. Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proc. 9th Int'l. Conf. Network Protocols (ICNP'01), Los Angeles, 2001, pp. 251–60.

