A SECURE CLUSTER BASED COMMUNICATION IN WIRELESS NETWORK USING CRYPTOGRAPHIC REPORTS

Hamsha1, Dr.Nagaraj2

Research Scholar[1] ,[1]Professor & Head of the Department,Computer Science,RVCE Bangalore

ABSTRACT

Mobile Adhoc Networks are becoming very popular in current Wireless Technology, which is been associated to business, socially and in some critical applications like Military etc, The network which is formed by self configuring wireless links which are connected to each other. These applications are categorized by hostile environment that they serve while communicating between nodes. However in such Wireless Network will be more exposed to different types of security attacks. The challenge is to meet secure network communication. In this paper we focus on cluster based secure communication to improve the reliability between clusters. In this scheme the Cluster Members (CM) submits a report to the Cluster Head (CH) and temporarily stores Evidences as a security tokens. The reports contain digital signatures. The CH will verify the consistency of the CM report and updates to Accounting Centre (AC). AC will verify the uniformity of reports and clears the cryptographic operations. For attacker nodes, the security tokens are requested to classify and expel the attacker nodes which submit wrong reports.

KEYWORDS

Selfishness, Security, Mobile Adhoc Network

INTRODUCTION

Security is one of the most crucial, when communicating between nodes. Implementation of security issues is a prime importance in wireless network [1][2].Wireless transmitters and receivers are equipped in MANETS nodes. The node parameters like transmission power level, co-channel interference level will change depending on the node locations. The topology will change with respect to the time when the node moves or adjust reception and transmission powers. Certificate management is one of the important roles in security issues in MANETS and this is widely used mechanism which serves as a public key infrastructure [3][4] for protecting the network applications. The processing of Certificate Management includes three phases: prevention, detection and revocation. Wide number of researches have been carried out in these areas [5][6][7][8][9][10]. Selfish nodes [11] which act as malicious nodes will drop the incoming packets (data packets and/or control packets) from the original nodes to minimize their energy levels, or forwarding their own data to the buffer queue. A selfish node degrades the MANETS performance to a great extent. Data transmission process will be corrupted, if the selfish node comes into existing and does not cooperate, which affects the overall network performance. The existing system, the credit card payment system is designed for threat models. In this procedure the initiator node and the intermediate nodes participate in packet forwarding using a transaction value, which is less than in a credit card payment scheme. Once the route is established, nodes involve in transactions, these transactions include low-value transaction, if route is broken, a new

DOI : 10.5121/ijnsa.2014.6504

transaction is established. Hence WSNs requires a payment scheme which is developed according to its characteristics. A secured reporting based scheme has to be effective, low overhead processing and less energy. The existing scheme has more communication overhead and complexity. The size of the security proof report is significantly large and uses the node resources and consumes more bandwidth. In this paper a cluster based report generation scheme is proposed. The clusters are formed and there is a Cluster Head (CH) which monitors the Cluster Members CM. Cluster Members (CM) submits a report to the Cluster Head (CH) and temporarily stores Evidences as a security tokens. The reports contain digital signatures. The CH will verify the consistency of the CM report and updates to Accounting Centre (AC). AC will verify the uniformity of reports and clears the cryptographic operations For attacker nodes, the security tokens are requested to classify and expel the attacker nodes which submits wrong reports

RELATED WORKS

Researchers have to pay more attention in implementing security issues in MANETS because of its changing topology, vulnerability and lack of infrastructure. Here we briefly discuss about cluster formation and types of clusters.

Voting based clustering

This mechanism invalidates the attacker report through votes from valid nodes. URSA [12] proposed the eviction of malicious node using voting based. The new joining nodes certificate is issued by the neighbouring nodes. The attacker node is evicted basis on the votes from its neighbouring. In URSA, the exchange of node information and node monitoring is performed by each node in one-hop. If the number of negative votes exceeds threshold value, the malicious node is evicted. Since nodes cannot directly communicate with other neighbour node without a valid certificate. The disadvantage of URSA is that, false malicious accusation will not be addressed.

Arboit et al. [13] proposed scheme, where all the participating nodes can vote together. There is No Certification Authority required. The participating nodes itself will monitor the activity and behaviour of neighbouring nodes. The nodes with variable weight vote in URSA method. Trustworthiness of the participating node is calculated as its weight.

Non-Voting-Based Mechanism

Clulow et al. [14] proposed self destruction of node strategy, in which malicious node behaviour can be revocated in one accusation. The attacker node is removed from the network by the accused node in the network. This approach also reduces the overhead of the node and this is limited. Disadvantage of this scheme is that, it does not differentiate from accused which falsely reports from original attacker nodes.

Park et al. [15] proposed a cluster-based certificate scheme, in which the CA is responsible for controlling and managing the accuser and accused nodes. The malicious node certificate can be revoked by any single participating node and also deals with the false proof detection of CM and can be moved to blacklist by CH

Existing (Tamper proof Devices) TDP [16][17][18][19] is one of the payment scheme used. In this scheme each participating node stores and manages its own credit account, hence secure its operations [20][21][22][23][24][25][26]. In offline mode, the participating nodes usually send wrong proofs to update Accounting centre (AC)

In SIP [17], the intermediate nodes update its credit rewards, after the data transmission between the destination and source nodes. When destination nodes sends RECEIPT packet to source to issue rewards.

ESIP [26] proposed payment scheme which uses a communication protocol. ESIP integrates limited hash function, public key cryptography and identity-based cryptography for massage transfer from source to destination. To secure payment, Message integrity is done using hash function and public key cryptography. To compute Source node and the neighbour node's symmetric key, Identity based cryptography is used. The hash value is generated at the source node and sends to intermediate node for message integrity check.

SYSTEM MODELS

Network Model

A Trusted Party (TP) maintains an Accounting centre (AC) for the credit updated by the Cluster Head, which is received by the Cluster Members. Here each cluster and Cluster members and has to register with the TP. TP assigns a one way symmetric key K_A and a certificate. This one way symmetric key is used for Intra cluster communication. For Inter Cluster communication Message Authentication Code (MAC) is used. When communication process take place between the nodes, the AC receives the report from nodes, and verifies for it consistency and fair reports. For the false report AC request for Evidences to distinguish between authentic and cheating nodes. Once the cheating node is identified, the CA denies renewing their certificates and evicts the node.

Cluster Model

Each cluster consists of Cluster Head (CH) and Cluster Members (CM), these cluster members are within CH communication range. CA is responsible for issuing certificates and authenticating the nodes which are participating in the network. When the node takes part in network, the node which is having high energy level is chosen as CH. CH propagates a REQUEST or a Hello Packet for periodic notification of neighbouring nodes. The CM which is within the transmission range can receive the request packet and CM replies with CM Hello packet to establish the connection with CH and joins the cluster. Later CH and CM will be periodically interacting using Hello Packets in time period T_u

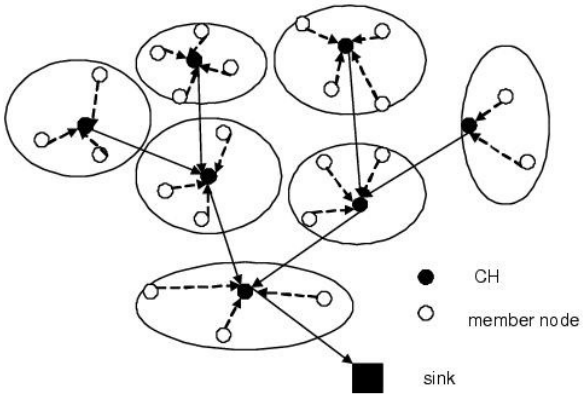

Figure 1: Cluster Formation

The above figure 1 show the cluster formation with Cluster Members (CM) and Cluster Head (CH) and these Cluster Members are within the range of Cluster Head.

Adversary Model

Trusted Party is highly and fully secured from the mobile node attacks. The attacker nodes are self controlled and non autonomous which leads to misbehave in network. Trusted Party monitors the network operation for secure communications. Without a Trusted Party it is difficult to analyse the secure report payments between nodes or entities. The attacker nodes can infer in cryptographic data and can also mislead node operations. The attackers can launch sophisticated attacks when they work individually or colliding with other nodes. [28] [29] [30].

IMPLEMENTATION

In our proposed system, it contains four phases. Communication phase, in which nodes communication is involved using sessions and Evidences and tokens as a security for authenticating nodes which submits in the form of report to Trusted Party (TP), Classifiers phase, involves in classifying fair and cheating reports. Identifying Cheating Nodes phase involves the Evidence request from the nodes to classify authentic and cheating nodes and eviction of cheating nodes and Account updating phase involves the updating the fair reports to the Accounting Centre for better communications.

Algorithm: Data transmission Evidence and Report

START
n_i is the source, intermediate, or destination node that is running the algorithm.
{
if (n_i is the source node) then
$P_X \leftarrow [R, X, Ts, M_X, Sig_S (R, X, Ts, H(M_X))]$;
send (P_X)
}
Else
{
if ((R, X, Ts are correct) and Verify (Sig_S (R, X, Ts, H (M_X))) = = TRUE) then
{
if (n_i is an intermediate node) then
Relay the packet;
Store Sig_S (R, X, Ts, H (M_X));
end if
}
}
{
if ($n_i$is the destination node) then
{
send ($h^{(X)}$);
}
}
end if
else
{

Drop the packet;
Send error packet to the source node;
}
end if
end if

if (P_X is last packet) then
{
Evidence = {R, X, Ts, H (M_X), $h^{(0)}$, $h^{(X)}$, H (Sig_S (R, X, Ts, H (M_X)), Sig_D(R, Ts, $h^{(0)}$))};
Report = {R, Ts, F, X};
Store Report and Evidence;
}
end if

STOP

Communication

This phase has four processes: route establishment, data transmission, Evidence Composition and report submission. In **route establishment**, an end-to-end route is established between source and destination. Source node broadcasts packets which contains parameters like (RREQ), Source ID, and Destination ID, time stamp and TTL. TTL specifies the number of intermediate nodes between source and destination. When the node receives the request packet, it claims its identity and broadcasts to its next intermediate nodes. The destination node replies with response packet for the broadcasted nodes and sends the packet to the source.

In **Data Transmission**, after route establishment from source and destination, the destination packet replies with the ACK packets. For the last data packet, the destination node appends the digital signature and sends the packet to the first node.

Evidence is the information of event or action proof occurrence, which occurred while establishing the route. The aim of the Evidence is to rectify the dispute about the digital signature resulted in data transmission.

The main functions of Evidences are:

- Evidences are unmodifiable
- If the source and destination nodes collude, they can create Evidences for any number of messages because they can compute the necessary security tokens.
- Evidences are unforgeable
- Evidences are undeniable

Submission of reports contains **session identifier**, which allocates the session for each transaction in which the node identities are concatenated and assigned time stamp. **Flag commands (F)** are used to acknowledge the transaction happened, the F (0) indicates the last received packet and F (1) for ACK **and message numbers (X).**

Node submitting report to TP contains Report Submission Packet at time t_i according to the sessionst_{i-1}. It contains details of last held session$[t_{i-1}, t_i]$, the node reports, time stamp and a

key K_A. The Aim of the TP is to assure secure communication without any manipulation of the reports which are sent by the authentic node.

Algorithm for submitting reports

$n_i \rightarrow$ TP: **Submit** (Reports $[t_{i-1}, t_i]$);
TP $\rightarrow n_i$: **Evidences_ Request** (Ses_IDs$[t_{i-2}, t_{i-1}]$));
$n_i \rightarrow$ TP: **Submits** (Req_EVS$[t_{i-2}, t_{i-1}]$);
TP: **Identify_Cheaters**();
TP: Clear the reports;
if (n_i is honest) **then**
{
TP $\rightarrow n_i$: Clearance for certificate;
}
end if

Classifiers and Identifying Cheaters

In this phase the cheating reports are identified and classified as fair and cheating reports. Below figure 2 shows the trusted party set up. The aim of proposed system is to identify the attacker node which leads to misbehave in the network and does not benefit the attacker node. The node which submits wrong reports are verified by AC asking evidences of the nodes for proof. If AC finds any incorrect information about digital signature and hash key of the node, the node is identified as cheater. Authentic node is verified by its Evidence which consist of proof generated by the node like signature and hash key, if this proof is similar to the Evidence proof, then the node is authentic.

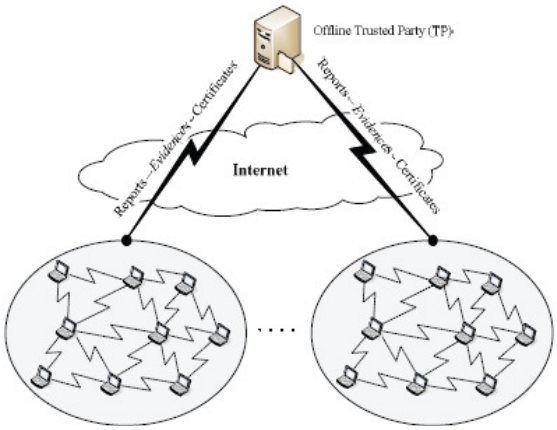

Figure 2: TP Managing Nodes in Network

PERFORMANCE EVALUATION

In this section we describe our simulation and Methodology as well comparing performance through simulation results of secured reports, Throughput, witness and Efficient Routing.

A. Simulation Methodologies

To differentiate between Authentic and Malicious Nodes. We simulate our proposed system using ns2 simulator.

B. Simulation Configurations

Our simulation is conducted with the Network Simulator (NS) 2.35 environment on a platform with GCC-4.3 and Ubuntu 11.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.35.

C. Random Key Generations

Random key is generated using cryptographic techniques, which generates 128 bit key length. This key is used for data communication and also for classifying between cheaters nodes which submits the wrong keys.

Below Table 1 show the parameter used to simulate the proposed system

SL No	Parameters	Values
1	Number of Nodes	49
2	Topology Dimension	1200x1200
3	Traffic Type	CBR
4	Radio Propagation Model	TwoRayGround
5	MAC Type	802.11
6	Packet Size	512
7	Antenna Type	Omni
8	Mobility Speed	250

Table 1: Parameters

Below Figure 3 Shows the Overall Data flow of the process.

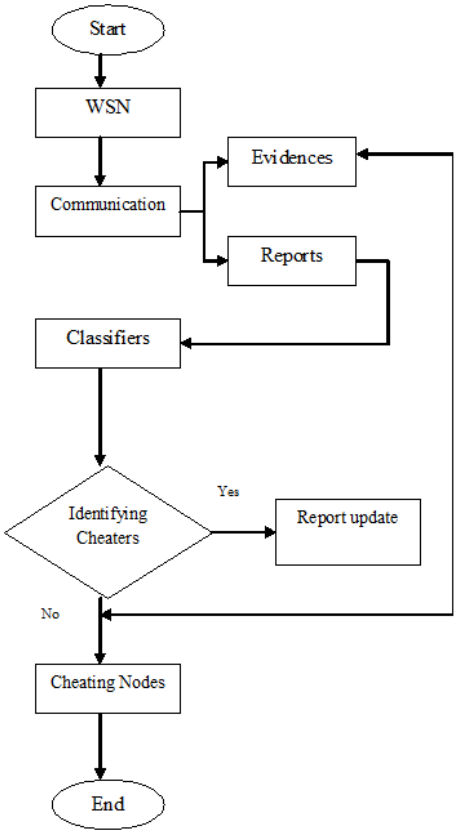

Figure 3: Flow Diagram

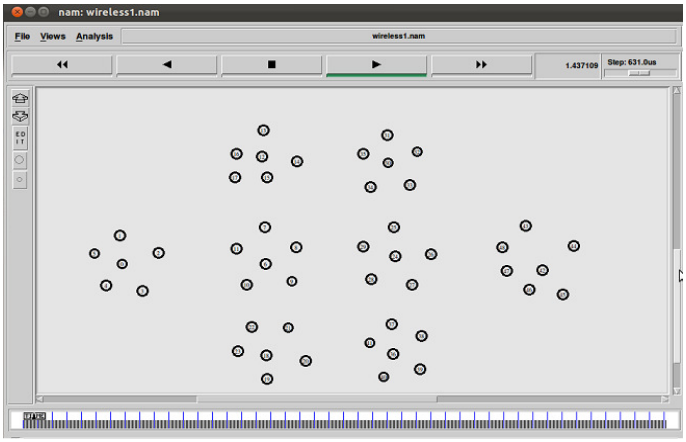

Figure 4: Cluster Formation

In the above figure 4, cluster is formed randomly. In each cluster number of nodes are six, in which one acts as the Cluster Head (CH) and others as Cluster Members (CM).

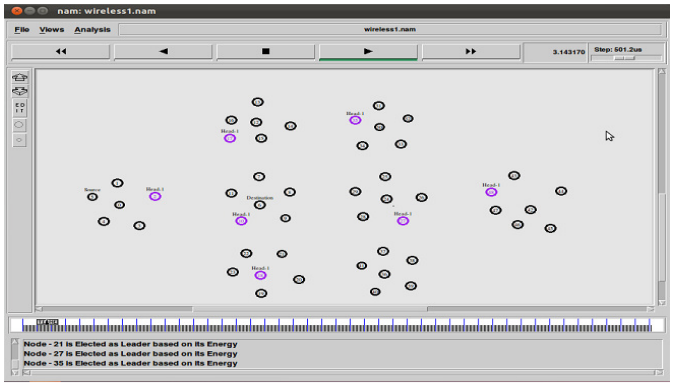

Figure 5: Cluster Head

Figure 5 shows the Cluster Head formation based on its energy level. The purple colour nodes indicates the cluster head, here 8 clusters are formed.

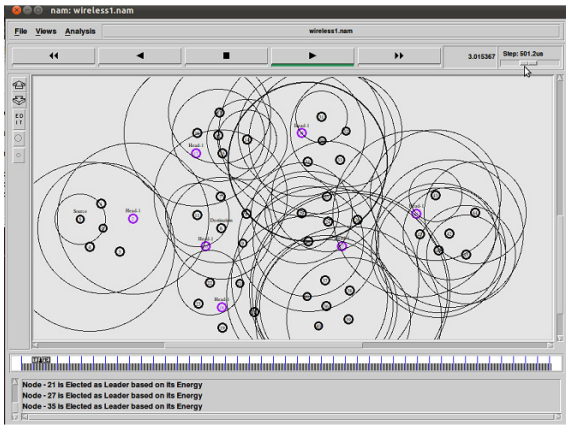

Figure 6: Node Communication

Above figure 6 shows the node communication using key. Source Node 5 sending data to destination node 6, through routeNode5→Node2 (CH1)→Node10(CH2)→Node6

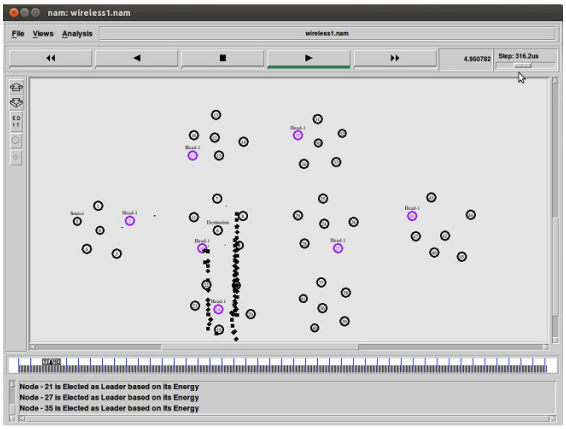

Figure 7: Malicious activity

In the figure 7, shows the malicious activity of nodes which is dropping the packets. Thus mismatching in keys and submitting wrong reports

SIMULATION AND RESULTS

1. Communication and Overhead

In secured communication the authentic nodes communicates with correct reports, thus reducing their node overhead by using light cryptographic techniques. In the below figure 8 the X axis indicates the time and Y axis indicates the Packet delivered. The green line indicates the node overhead, which tries to manipulate report and does some malicious activity like packet drop. Whereas Red line indicates our approach which submits report and by reducing node overhead.

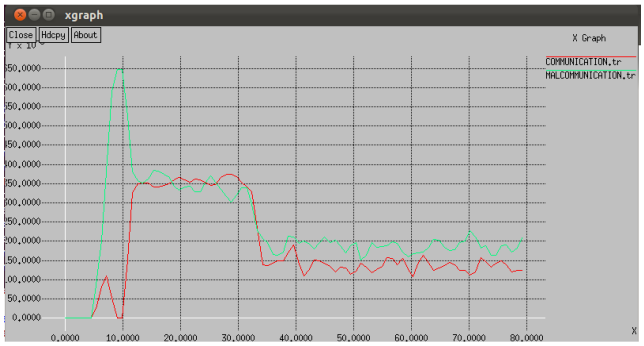

Figure 8: Node Communication Overhead

2. Node Witness

In the below figure 9 shows the node submitting the correct reports to AC, increasing throughput by delivering the packets. Here we can analyse our proposed system, in which the node submits the correct report and it is witness by Trusted Party. Here the red line indicates the correct report submitted. There is a variation in the peaks indicating the submission of correct report. If the red line goes flat, it indicates the node is evicted. X axis indicates the timings and Y axis indicates node submitting report for witnessing.

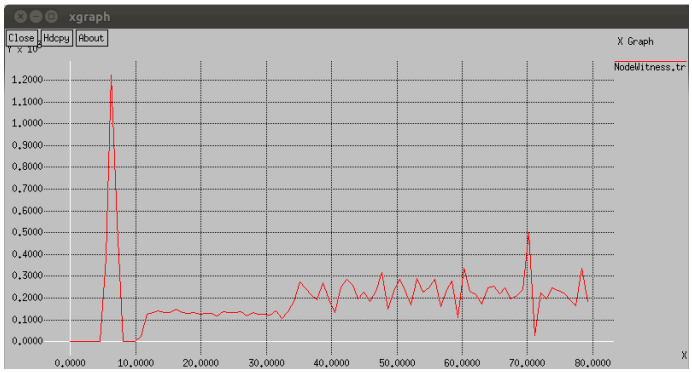

Figure 9: Node Throughput

CONCLUSION

In this approach a report based submission to AC is defined to classify the fair and cheating nodes. The report based decreases the node overhead by reducing the cryptographic operations. In case of cheaters nodes the Evidences is requested and processed. Our simulation result shows the node process low overhead communication for submitting fair reports.

FutureEnhancement:-Cryptographic technique can be used for multiple sink nodes.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007

[3] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[6] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.

[7] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

[8] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[9] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.

[11] Matthias Hollick, jens Schmitt, Christian seipl,..On the Effect of Node Misbehaviour in Ad hoc Network. IEEE conference ,vol 6, pp 3759 . 3763, 2004.

[12] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.

[13] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008

[14] J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006

[15] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

[16] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

[17] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 569-582, Oct. 2007.

[18] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.

[19] A. Weyland, T. Staub, and T. Braun, "Comparison of Motivation- Based Cooperation Mechanisms for Hybrid Wireless Networks," J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

[20] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.
[21] M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.
[22] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.
[23] M. Mahmoud and X. Shen, "Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc. IEEE INFOCOM '10, Mar. 2010.
[24] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.
[25] J. Pan, L. Cai, X. Shen, and J. Mark, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," Computer Networks, vol. 51, no. 3, pp. 853-865, 2007.
[26] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011
[27] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks," IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489, Dec. 2007.
[28] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.
[29] M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.
[30] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

Biblography

Hamsha.k
BE Computerscience,
MS,BITS PILANI,M.Tech,CS,(Ph.D)
Area:Security and Networking.