Location Aware Clustering and Trust Management in Mobile Ad Hoc Networks

Michail Chatzidakis and Stathes Hadjiefthymiades
Department of Informatics and Telecommunications
National and Kapodistrian University of Athens

***Abstract*—Properly clustering a Mobile Ad Hoc Network (MANET) is an efficient method to ensure optimal network resources exploitation. A lot of clustering schemes have been proposed, most of them suffering from the same drawback i.e., cluster lifetime instability due to the mobility of the nodes. In order to cope with this particular problem, along with trust issues that arise and have been partially investigated previously, we propose a time-optimized clustering scheme which improves the lifespan of the network clusters, thus leading to increased trust efficiency, since malicious nodes are easier to locate. The malicious node spotting is achieved by combining individual node observations, as well as the collective cluster trust estimation regarding the reputation vector of a specific node.**

***Index Terms*—Trust Models, Security Models, Protocol Design, Network Security, Intrusion Detection**

I. Introduction

Wireless networks have become increasingly popular since late '90s, when IEEE 802.11 specification (Wi-Fi) was introduced and later refined [1]. Since then, a variety of wireless networks have been deployed, ranging from small Wireless Personal Area Networks (WPANs), e.g., a bluetooth network between a wireless headset and a mobile phone, up to Wireless Wide Area Networks (WWANs), which cover large areas, such as neighboring towns and may use optical fibers, microwaves or even satellite links. Cellular networks are another example of wireless networks, which cover large areas utilizing base stations, creating a cell adjacent to other cells, monitored by different base stations. Care has been taken so that adjacent cells do not transmit/receive at the same frequency [2].

A mesh network utilizes a topology that assumes the existence of nodes which can relay data to other nodes acting as routers or gateways. It is based on the cooperation of the nodes for the transmission of the information through the network. Mesh topology can be applied to either wired and/or wireless networks.

A Mobile Ad Hoc Network (MANET) is essentially a wireless mesh network with the added complexity of the mobility of all of the nodes of the network. There are no base stations, nor any predefined topology. The nodes that are part of the network are mobile and autonomous, equipped with their own power bank, receiver, transmitter, computing capabilities, memory modules and are often equipped with a variety of sensors which collect information from the environment and transmit it accordingly.

In order for the entire MANET network to operate efficiently and securely, two key factors must be addressed:

- An efficient power management scheme should be adopted, which will maximize the operation of the entire network and
- A trust mechanism should be applied, which will ensure that any malicious nodes will be quickly spotted and isolated from the rest of the network.

This paper addresses both of these issues. We propose a clustering scheme, a modified version of the Cost of Analysis concept [3], for the Cluster Head (CH) election. We propose that the cluster persistence should be affected only by the nodes that, at the beginning of the cluster formation, have a positive impact to cluster cohesion, i.e., their distance from the CH decreases. This substantially improves cluster stability.

We also propose a trust/reputation management scheme, which will allow the nodes to evaluate the trust of other nodes, prior to proceeding with actual data exchanging. This is done by the client node part, which takes into account the reputation vector of the potential server node, stored on the CH. The CH's reputation vector integrates all of the preceding trust evaluations for the potential server node and is essentially a cluster collective reputation metric. Following the CH's opinion and in regards to a trust threshold that can be node specific, the transaction may be carried on, or canceled accordingly.

The rest of the paper is organized as follows: Section II describes previous work that has been done in the field while section III describes how a cluster is formed. Section IV describes our simulation results and section V presents the conclusion of our work. Finally we present our plans for future work in section VI.

II. Previous Work

A. Network Security

In regards to network security, a common approach is to deploy a third party Certificate Authority (CA). Most commonly the X.509 standard [4], as well as kerberos [5] is used. The drawback of these approaches is that a centralized CA is not always feasible to be present in a MANET as a physical entity. Moreover, cryptographic key management in a MANET is a challenge and although there is some progress in the field, i.e., [6], there are still a lot of problems to be solved, mainly in the power management of the CA as well as the distributed character of such an entity as shown in [7]. A distributed approach to the clustering problem is presented in [8].

Several studies are dealing with trust issues in networks in general [9]–[18], yet, the application to MANETs is not always feasible.

B. Clustering

A classification of clustering algorithms can be found in [19] and [20]. As shown, there are several factors that have to be considered in order to efficiently cluster a MANET. However, despite the variety of the algorithms, all of them have one thing in common: they are all designed targeting the efficient exploitation of the network resources. In most cases, the clusters formed have a short lifespan and that is a common drawback of the all clustering schemes.

Every clustering scheme proposes the existence of a Cluster Head node (CH), which is a node running Intrusion Detection System software (IDS), maintains routing and trust information and, as a result of these activities, is rapidly consuming its power resources. In order to motivate the nodes to act as CHs, a CH reward scheme has been proposed in [3], which compensates the CH with future privileges such as increased bandwidth and service priority. In this work, the Cost of Analysis (CoA) is introduced, which is actually a function that we, too, adopt (as Cost of Analysis/Processing –CoA/P), since it has been proven to be a reliable and secure way of broadcasting the ability of a node to serve the cluster as a CH, without revealing sensitive information about the status of specific node resources parameters, such as the node's power status [3]. In the opposite case (i.e., if the power level and/or the computational capabilities of the node is revealed), the node could potentially become a target of adversaries trying to attack it and corrupt the whole network.

From a game-theoretic approach, nodes are motivated to transmit their true CoA/P since the opposite behavior leads, in the long term, to node isolation and/or energy drain due to low priority in service and limited bandwidth [3].

In [21], the persistence of a group of nodes is exploited, in order for information to be transmitted only to one of the nodes which will, in turn, share the acquired information with the rest of the group. This minimizes network traffic (node to base station and vice versa) and information overhead, while maintaining the nodes up to date. Such a Location Based Services application (LBS) on moving nodes is especially useful in the case of vehicles which tend to move with similar speed to the same direction.

C. Trust

A thorough review of trust management schemes can be found in [22]. In these schemes, the trust of each node is evaluated either directly, i.e., by observing the behavior of the node in question by the interested node, or indirectly, by trust management information that is either accumulated in the form of a reputation vector in a CH buffer, or by means of specific nodes that observe the behavior of other nodes (watchdogs). In all scenarios the importance of collecting information in a distributed manner is dominant.

Our previous work [23] provided an intrusion detection mechanism, along with a trust management scheme to locate malicious nodes. However, it didn't address the cluster limited lifetime problem. We address this issue in the present work.

III. Cluster formation

Clustering a MANET is a method for uniform exploitation of network resources, as shown in [24]. In the opposite case, if a threshold number of nodes run out of energy, the network is prone to stop functioning, although many nodes may still have adequate power and other resources left. A sophisticated resource consumption plan will increase the lifespan of the network along with its efficiency and credibility.

We used a java simulation to set up a MANET with nodes moving in a rectangle field (1000×1000) following the Random Waypoint pattern. Each node is powered by a power unit, is equipped with a Global Positioning System module or similar equipment, in order to be able to determine its exact location on the field. The nodes are uniquely identified by an ID number and are able to transmit information using a transceiver, up to a certain range (100). Cryptography schemes may or may not apply, depending on the nature of the MANET and the available computing resources. In our simulation, no cryptographic scheme was applied.

A. Transactions Between Nodes

In order for a client node i to proceed to a transaction (data exchange) with a server node j, certain trust criteria must be met. There are two parameters which are of great importance to every computer network, namely Reputation R and Trust T. We define

- Reputation R_{ij}: is a float number in the $[0, 1]$ range which reflects the opinion that node i has, regarding node j and is formed from observations of previous transactions and a weighted consultation of the reputation vector kept by the CH. The closest to 1, the more reputable node j is.
- Trust T_{ij}: is, too, a float number in the $[0, 1]$ range, which reflects the anticipated behavior of the node j for a certain transaction that node i is willing to initiate. It is related to R_{ij} and, again, values close to 1 indicate a strong probability that node j is expected to behave in a non-malicious manner.

In short, R_{ij} refers to the i node's past observations of the behavior of node j and is thus a non disputable metric, while T_{ij} refers to the expected future behavior of node j and is associated with the transaction trust policy of node i that makes the prediction. Depending on node i, a trust T_{ij} value above a certain threshold, set by i, will lead to an initiated transaction, while a T_{ij} below the node's i threshold will cause the client node i to abort the transaction following by CH notification, to incorporate the event to node's j reputation vector coordinate.

B. Reputation and Trust Vectors

Each node maintains two reputation vectors, the Local Reputation Vector (LRV), reflecting the reputation R for all other nodes and the Global Reputation Vector (GRV) which stores the same piece of information when the node acts as a CH. The main difference between these two vectors is that LRV coordinates are estimated both by direct observation of the target node and weighted consultation from the CH, while GRV's coordinates are built up from the observations of all cluster nodes and reflects the collective reputation estimation of the cluster regarding node j.

C. Cost of Analysis/Processing

As already stated, an efficient method of fully and uniformly exploiting the entire network resources, is clustering the network and elect a node, with adequate resources, to act as a Cluster Head (CH) for each cluster. The node that acts as a CH is consuming its resources in a higher rate than the cluster members, as it is under a heavy load of work (communicating with all the cluster members, running IDS, frequently updating its reputation vector). However, the motivation to undertake those additional tasks is a reward scheme which will give the CH serving priority in the future when new clusters will be formed. Following [3] we first define the percentage of sampling PS_i as

$$PS_i = \frac{R_i}{\sum_{k=1}^{N} R_k} \tag{1}$$

where R_i is the reputation of the node and $\sum_{k=1}^{N} R_i$ is the total reputation of the nodes in the network that appear in the node's LRV. The percentage of sampling as defined in eq. 1 is essentially the relative reputation of the node in question.

The power factor of a node PF_i of a node i is

$$PF_i = \frac{E_i}{nT_i} \tag{2}$$

where E_i is the energy of the node, n is the number of the expected time slots that the node is willing to act as a CH and T_i is the actual duration of each time slot. The PF indicates the energy per clock count that is required from the CH, for the anticipated cluster operation. The MANET is not homogeneous, so not all of the nodes have the same energy level, nor all of the nodes are willing to act as a CH for the same number of time slots. This leads to a node-specific PF.

Taking into account eq. 1 and eq. 2, the cost of analysis/processing function (CoA/P) is then defined as

$$c_i = \begin{cases} \infty & \text{if } E_i < E_{ch} \\ \frac{PS_i}{PF_i} = \frac{\frac{R_i}{\sum_{k=1}^{N} R_k} \times nT_i}{E_i} & \text{otherwise} \end{cases} \tag{3}$$

where E_i is the node's energy and E_{CH} is the minimum energy required for the operation of the cluster. CoA/P c_i does not reveal sensitive information about the node, yet it is a measure of the node's capability to act as a CH. Following eq. 3, a node that does not have enough resources to act as a CH, will have $c_i = \infty$ and, thus, will declare its inability to act as a CH. On the other end, small values of c_i are a strong indication that the node in question is able to act as a CH.

D. Cluster Head Election Phase

The CH is elected by its 1-hop neighbors. Every node broadcasts its CoA/P c_i and the one with the lowest c_i is elected as CH. All the nodes that voted for it and thus are 1-hop away from the CH, become Cluster Members (CM). This inevitably results to 1-hop clusters and prevents cluster overpopulation. However, once the cluster is formed, a node can continue to exchange data with other CMs even if the node is, temporarily, out of CH range. A node that is beyond CH's broadcasting range can not initiate a transaction. It can merely finish one that has already started.

There are three cases that a CH election is initiated:

- At the beginning of the MANET's operation.
- When a cluster is considered fragmented according to some specific criteria which are discussed bellow.
- When a CH's energy drops under a certain threshold which is CH-specific and the CH consequently quits.

E. Payment Scheme

When a node acts as a CH, its resources are rapidly consumed, due to the increased information flow between the CH and the CMs. To compensate for this increased power consumption, a form of payment is established and the CH gets higher priority to the transactions that follow. A lot of payment schemes have been proposed. We adopted the one discussed in [3, p. 94]

$$P_k = \sum_{i \in N} vt_k(C, i) B \rho_k \tag{4}$$

with

$$\rho_k = c_k + \frac{1}{\sum_{i \in N} vt_k(C, i)} \times \left[\sum_{j \in N} \sum_{i \in N} vt_j(C | c_k = \infty, i) - \sum_{j \in N} c_j \sum_{i \in N} vt_j(C, i) \right] \tag{5}$$

where
P_k is the payment of k node,
$vt_k(C, i) = 1$ if node i votes k node, otherwise $vt_k(C, i) = 0$,
B is the cluster-head budget (packets per time unit),
ρ_k is k nodes payment per packet,
c_k is k's node cost of analysis/processing
C is the network's cost of analysis/processing vector.

With this payment scheme, the nodes are motivated to declare their true CoA/P without revealing sensitive information (e.g., their power or memory status, computing capabilities etc.) [3]. Note that eq. 4 and eq. 5 are given for reference only.

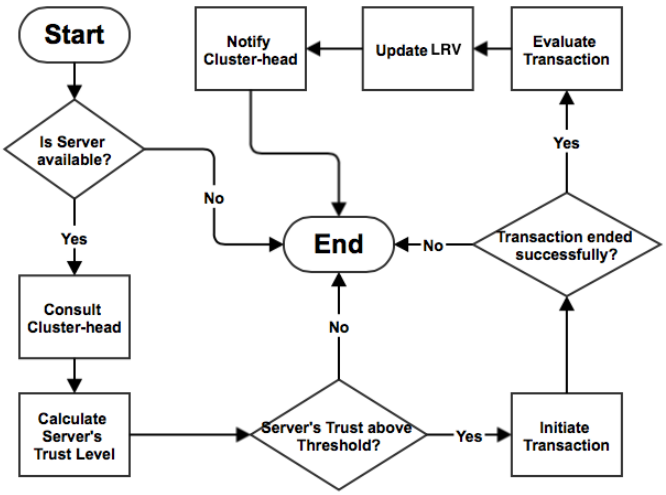

Fig. 1. Transaction flowchart

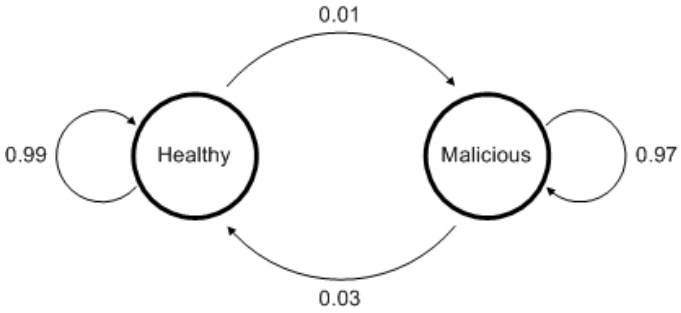

Fig. 2. Healthy/Malicious Markov chain

F. Cluster Persistence

Let $\vec{r_i}$ be the distance vector from the CH to the i node. If $\Delta|\vec{r_i}| \leq 0$, the persistence of the cluster increases, while if $\Delta|\vec{r_i}| > 0$, the persistence of the cluster decreases. By taking into account only the nodes that, during the cluster formation phase, contribute positively to the cohesion of the cluster, the CMs are divided into two categories. Those which have a positive impact to the cluster cohesion and those whose contribution to the cluster cohesion is negative. By considering only the first set of nodes, i.e., those who tend to minimize $\sum_i |\vec{r_i}|$, we show by simulation that the clusters created are more consistent and time persistent, thus solving a fundamental problem of network clustering in MANET.

G. Trust Evaluation and Transaction Mechanism

The trust evaluation mechanism has been discussed in [23]. However, we modify our approach to clarify the difference between reputation and trust.

Each node's LRV reflects the opinion of the node for the behavior of the rest of the nodes of the network, at a given time instance t. When a node i, acting as a client, requires a transaction with node j, acting as a server, it first consults the CH. The CH's estimation of the reputation, regarding node j, is transmitted to node i with a message $CH_{rep}(i,j,t)$ and is merged with node's i reputation for node j, as shown in eq. 6:

$$T_{ij} = LRV(j,t) = e \times CH_{rep}(i,j,t) + (1-e) \times LRV(j,t-1) \quad (6)$$

where e is the weighing factor which is node-specific. Thus, the trust T_{ij} of node j is estimated.

If $T_{ij} \geq T_{thr}$, T_{thr} being the trust threshold of node i, the transaction is initiated. After the end of the transaction, it reports to the CH its verdict about the behavior of node j, at a certain time t, in a message $T_{rep}(i,j,t)$. In the opposite case, i.e., $T_{ij} < T_{thr}$, the transaction is aborted.

The CH collects all the information from the CMs and integrates it to its GRV as follows from eq. 7

$$GRV(j,t) = \alpha \times \frac{\sum_{i=1}^{n} T_{rep}(i,j,t)}{N} + (1-\alpha)\, GRV(j,t-1) \quad (7)$$

where α is CH's weighing factor in the range $[0,1]$. It expresses the behavior of the CH. A "selfish" CH would have an α factor at the vicinity of the lower bound of the range and vice versa. The α parameter can also be chosen as a function of time (i.e., $\alpha = f(t)$), so as to reflect the information aging, since the information context is time variant and older information may be less important than new one.

The whole procedure of a transaction is shown in fig. 1.

IV. Results

Using mobisim [25], we created trace paths for various scenarios. We developed a Java simulation for the scenarios and, using the traces as input to our simulator, we created a square field with dimensions $1000m \times 1000m$ and various numbers of mobile nodes (i.e., $20, 30, 40, 60, 80, 100$), which move following the Random Way-point pattern. The node velocities were uniformly distributed in the range $[0, 10ms^{-1}]$. The healthy-to-malicious and malicious-to-healthy transition is shown in fig. 2 along with the transition probabilities. The transceiver range of the nodes is $100m$ and the node's initial energy follows the Gauss distribution in the range $3,000$ to $4,000$ energy units. The energy cost of a transactions is 1 energy unit per packet and a node that exhibits malicious behavior gets 0.5 penalty to its reputation R by the client node, while this penalty is also announced to the CH to update the GRV component accordingly.

We repeatedly run every scenario with random initial conditions, both for low (i.e., velocities that fall in $(0,1)$ range and high mobility nodes (i.e., velocities that fall in $(0,10)$ range. We showed that, considering the results from previous work [23], the clusters were much more stable, up to two orders of magnitude.

The number of elections, which induce a significant computational cost, was reduced, while the cluster lifespan was lengthened. Moreover, due to the lengthening of the lifespan of the cluster, the nodes were able to complete time-consuming transactions that were not possible before.

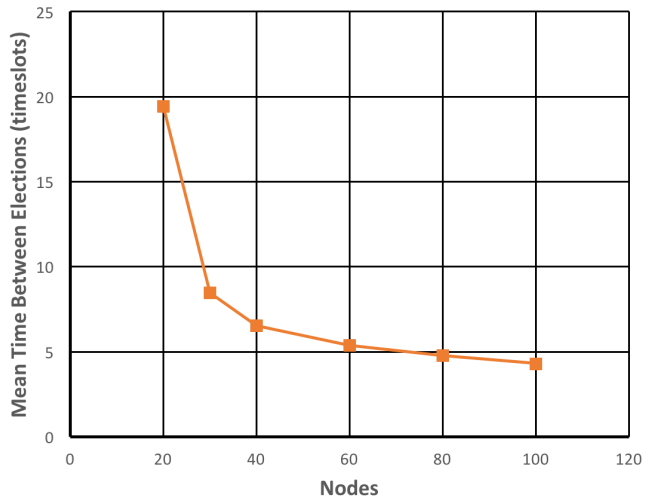

Fig. 3. Mean time between elections for high mobility nodes

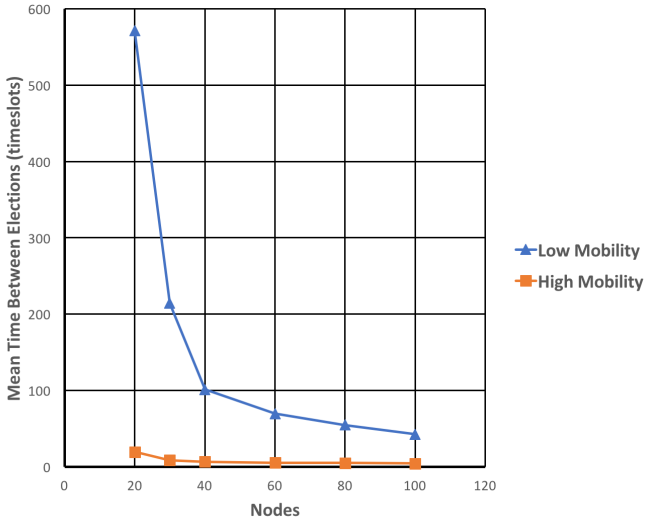

Fig. 4. Mean time between elections for high and low mobility nodes

The high mobility scenario is shown in fig. 3. For reference purposes, both of the scenarios are shown in fig. 4 together, which makes clear that the low mobility scenario has much more to benefit from the proposed scheme.

When a CM spots a node exhibiting malicious behavior, it reports it to the CH for a proper update to the corresponding GRV component, so that, when other nodes request a transaction with the malicious node, they may take that information into consideration, as described in III-G. This information is passed down to the nodes, but it is up to the client node to decide whether it will proceed with the transaction or not. More specifically, a CM node with low trust threshold, may continue and have a transaction with a potential malicious server node, while some other nodes may avoid the risk.

As an additional fail-safe measure , when a node has been previously characterized as malicious, its trust may be restored by the CH if there are indications that the node is non-malicious any more and thus continue to contribute to the network functions.

By simulation we found that the percentage of malicious node transactions is independent of the number of nodes in the low mobility scenario and is around 10% as shown in table I, as expected in accordance with the markovian transition probability (i.e., 10%), but it seems to decrease substantially in the high mobility scenario as shown in table I and fig. 6 dropping down to 5.98%. The data collected are shown in fig. 5, fig. 6 and table I, where the number of successful transactions and percentage of malicious transactions are shown.

V. Conclusion

The main goal of our work was to show that the cluster stability increases, when CH elections are held only when a node that initially contributed to the cohesion of the cluster, falls out of CH's communication range. We showed that the lifespan of a cluster is increased drastically (by two orders of magnitude, in regards to our previous work) and that this has a positive impact to the percentage of malicious transactions especially in the high mobility scenario. We showed that

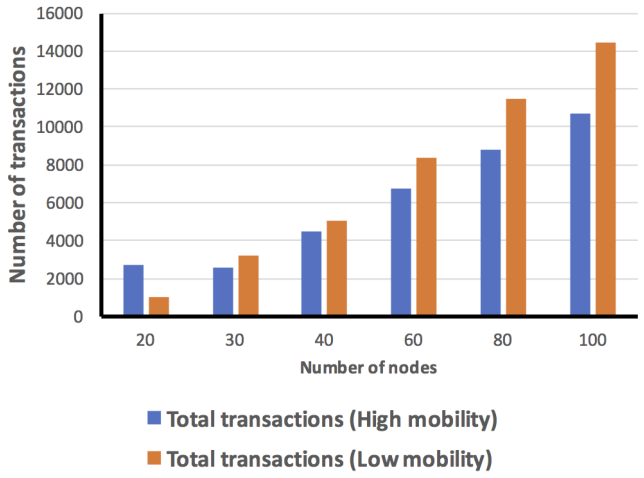

Fig. 5. Total number of transactions

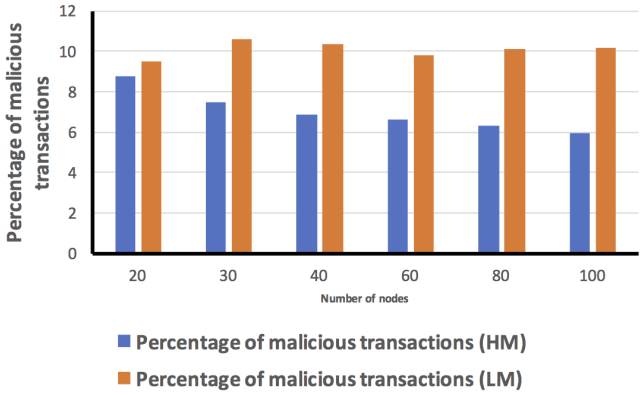

Fig. 6. Percentage of malicious transactions

TABLE I
PERCENTAGE OF MALICIOUS TRANSACTIONS

Node No	Percentage of malicious transactions High Mobility	Percentage of malicious transactions Low Mobility
20	8.74	9.5
30	7.46	10.6
40	6.86	10.36
60	6.62	9.82
80	6.3	10.08
100	5.98	10.16

the low mobility scenario benefits from the increased cluster lifespan, but the great benefit is in the high mobility scenario where the information of the status of a node did not have adequate time to spread throughout the cluster. In fact the malicious transactions number decreases more than 40% as shown in table I.

VI. FUTURE WORK

Our plan is to further improve this particular scheme, in order to reduce the response time to a malicious node and improve the time persistence of the clusters. We also intend to explore the role of the a and e weighing factors, to observe how a selfish behavior affects the network operation. It is obvious that the time that a particular trust value was assigned to a node, is crucial regarding the anticipated behavior of the node. In this direction we plan to investigate the a and e dependence of time, thus introducing the concept of information aging and fine tune the above proposed scheme.

REFERENCES

[1] IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) , vol., no., pp.1-2793, March 29 2012

[2] Guowang Miao, Jens Zander, Ki Won Sung, Ben Slimane: Fundamentals of Mobile Data Networks, Cambridge University Press 2016, ISBN 1107143217

[3] Mohammed, N., Otrok H., Wang, L., Debbabi, M. and Bhattacharya P.: Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET, IEEE Transactions on Dependable and Secure Computing, vol 8, No. 1, January - February 2011

[4] PKIX Working Group: Internet X.509 Public Key Infrastructure, 2007. Draft-ietf-pkix-rfc3280bis-08.txt

[5] C. Neuman, T. Yu, S. Hartman, and K. Raeburn: The Kerberos network authentication service, Ver. 5, Jul. 2005. RFC 4120.

[6] Saju P John, Philip Samuel: Self-organized key management with trusted certificate exchange in MANET, Ain Shams Engineering Journal, Volume 6, Issue 1, 2015, Pages 161-170, ISSN 2090-4479

[7] P. Xia, M. Wu, K. Wang and X. Chen, "Identity-Based Fully Distributed Certificate Authority in an OLSR MANET," 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, 2008, pp. 1-4. doi: 10.1109/WiCom.2008.614

[8] C. R. Lin and M. Gerla, "A distributed architecture for multimedia in dynamic wireless networks," Global Telecommunications Conference, 1995. GLOBECOM '95., IEEE, 1995, pp. 1468-1472 vol.2. doi: 10.1109/GLOCOM.1995.502646

[9] A. Jøsang and S. Pope: Semantic constraints for trust transitivity, in Proc. 2nd Asia-Pacific Conf. Conceptual Model., Jan. 2005, vol. 43, pp. 59–68.

[10] T. Repantis and V. Kalogeraki: Decentralized trust management for ad hoc peer-to-peer networks, in Proc. 4th Int. Workshop Middleware for Pervasive Ad-Hoc Comput., Nov. 2006, vol. 182, p. 6.

[11] A. Jsang, R. Ismail, and C. Boyd: A survey of trust and reputation systems for online service provision, Decision Support Systems, vol. 43, no. 2, pp. 618–644, Mar. 2005.

[12] J. Liang, N. Naoumov, and K. W. Ross: The index poisoning attack in P2P file sharing systems, in Proc. IEEE INFOCOM, Apr. 2006, pp. 1–12.

[13] P. R. Zimmermann: The Official PGP User's Guide. Cambridge, MA: MIT Press, 1995.

[14] S. Buchegger and J. L. Boudec: Performance analysis of the confidant protocol: Cooperation of nodes—Fairness in dynamic ad hoc networks, in Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput., Jun. 2002, pp. 226–236.

[15] P. Michiardi and R. Molva: Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in Proc. IFIP TC6/TC11 CMS, Sep. 2002, pp. 107–121.

[16] G. Theodorakopoulos and J. S. Baras: Trust evaluation in ad hoc networks, in Proc. ACM Workshop Wireless Security, Oct. 2004, pp. 1–10.

[17] Y. Sun, W. Yu, Z. Han, and K. J. Liu: Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305–317, Feb. 2006.

[18] D. Gambetta, Trust: Making and Breaking Cooperative Relations. Oxford, U.K.: Blackwell, 1988, ch. 13, pp. 213–237

[19] Agarwal, R., Motwani, M.: Survey of clustering algorithms for MANET. International Journal on Computer Science and Engineering Vol.1(2), 2009, 98-104

[20] Boyinbode, O., Le H.,Mbogho A.,Takizawa M. and Poliah R.: A Survey on Clustering Algorithms for Wireless Sensor Networks, 2010 13th International Conference on Network-Based Information Systems, Takayama, 2010, pp. 358-364. doi: 10.1109/NBiS.2010.59

[21] Anagnostopoulos, C., Hadjiefthymiades, S., Kolomvatsos, K.: Time-optimized user grouping in Location Based Services, Computer Networks 81 (2015) 220 - 244

[22] Cho, J. H., Swami A. and Chen I. R.: A Survey on Trust Management for Mobile Ad Hoc Networks, IEEE Communications Surveys and Tutorials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011. doi: 10.1109/SURV.2011.092110.00088

[23] Chatzidakis, M. and Hadjiefthymiades S.: Trust management in mobile ad hoc networks, 2014 16th International Telecommunications Network Strategy and Planning Symposium (Networks), Funchal, 2014, pp. 1-6. doi: 10.1109/NETWKS.2014.6958525

[24] Basagni, S.: Distributed Clustering for Ad Hoc Networks, Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms and Networks

[25] Mousavi, S. M., Rabiee, H. R., Moshref, M., and Dabirmoghaddam, A. 2007. MobiSim: A Framework for Simulation of Mobility Models in Mobile Ad-Hoc Networks. In Proceedings of the Third IEEE international Conference on Wireless and Mobile Computing, Networking and Communications (October 08 - 10, 2007). WIMOB. IEEE Computer Society, Washington, DC, 82.