# Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks

Moazam Bidaki[1] and Mohammad Masdari[2]

[1]*Department of Computer Engineering, Neyshabur Branch, Islamic Azad University, Neyshabur, Iran*

[2]*Department of Computer Engineering, Urmia Branch, Islamic Azad University,*
[1]*Bidaki@Iau-neyshabur.ac.ir,Urmia, Iran,* [2]*M.Masdari@Iaurmia.ac.ir*

***Abstract***

*Clustering is one of the main techniques that are used to increase the scalability of MANETs, but without any security considerations clustering is prone to various security attacks. Some cryptographic-based schemes have been proposed to secure the clustering process, but they are unable to handle the internal attacks. Trust-based clustering schemes have combined the trust management systems with the existing state of art clustering solutions and using cryptographic mechanism these schemes present the most complex and secure clustering solutions that are resilient against both internal and external attackers. In this paper, we present an in-depth analysis of trust-based clustering schemes and illustrate how reputations are integrated in these schemes. Then we compare them based on the various trust metrics and finally conclude with open research issues.*

***Keywords:*** *Direct Trust, Indirect Trust, Security*

## 1. Introduction

Clustering divides the network nodes into different virtual groups which are geographically adjacent and helps to organize the ad hoc networks hierarchically. A great number of heuristic clustering algorithms have been presented in the literature and in [1] Yu *et al.*, discuss about the latest developments in clustering and categorize the existing clustering schemes as dominating-set based clustering, low-maintenance clustering, mobility-aware clustering, energy-efficient clustering, load-balancing clustering and combined-metrics-based clustering.

Also, in [2] Wei *et al.*, classify the clustering schemes as single hop VS multi-hop schemes and location-based VS non-location-based schemes and stationary VS mobile schemes and asynchronous VS synchronous schemes. In addition, they analyze each category and illustrate their advantages and limitations. Although, numerous survey papers [3-9] have studied the existing clustering solutions, none of them have investigated the security issue. Because of special characteristics of wireless communications and MANETs, clustering algorithms are vulnerable to numerous passive and active security attacks. Therefore, we can categorize the clustering algorithms against their security features. Figure 1, shows the classification of clustering schemes from security perspective into secure and insecure solutions. Numerous insecure clustering algorithms have been presented for MANET and almost all of them assume that network is operating in trusted and secure environment or simply they ignore the security issue. Consequently, these schemes cannot protect the clustering process against malicious internal nodes and external attackers.

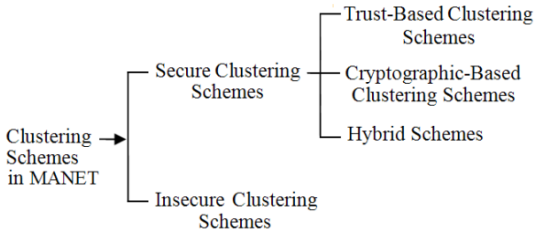


**Figure 1. Classification of Clustering Schemes**

Thus we need secure clustering solutions which are resilient to the various security problems of MANET and provide secure and reliable clustering even at the presence of malicious nodes and attackers. Some cryptography-based clustering schemes such as [10-13] have been designed for MANETs which are able to operate in hostile environment and use PKI or symmetric encryption techniques, but they do not offer sufficient protection against insider attackers and compromised nodes. To solve these problems, the notion of reputation should be used to detect and isolate the misbehaving nodes in the network. Trust-based clustering algorithms integrate the trust management systems with clustering algorithms to decrease the overheads of reputation management. The growing interest in the reputation-based systems inspired numerous trust-based clustering schemes for MANETs. But to the best of our knowledge, despite the high number of these algorithms [3-9], no survey paper has studied reputation-based security in clustering algorithms. In this paper, our contribution is to present an in-depth discussion and analysis about the well-known trust-based clustering schemes and clarify their features, capabilities and advantages. This study can be very helpful in understanding the limitations of existing solutions and designing new clustering schemes which can be resilient against various misbehaving. The rest of this paper is organized as follows: Section 2 discusses about the trust management systems in mobile ad hoc Networks. Section 3 illustrates CH selection algorithms in proposed trust based clustering schemes and Section 4 analyzes the cluster management operation of each scheme and determines their advantages and disadvantages in detail.

## 2. Security Attacks

Due to the wireless communication and dynamic nature of mobile ad hoc networks, various attacks can be launched against any layer of the protocol stack in these kinds of networks. Figure 2 shows the classification of attackers and their countermeasures in MANETs. Generally, attackers can be classified into insider and outsider ones. An external attacker is not a legitimate node and does not belong to the network, but an internal attacker is an authorized and valid MANET node. Furthermore, each type of attackers can launch many kinds of active and passive attacks. In passive attacks, the attacker can only eavesdrop or monitor the network traffic [14, 15].

### 2.1. Trust Management Systems

To enhance the security of MANETs and prevent malicious misbehaviors, it is important to evaluate the trustworthiness of nodes. To do this, it is necessary to use a trust management framework to collect reputation from all over the network and only provide service to trusted nodes.

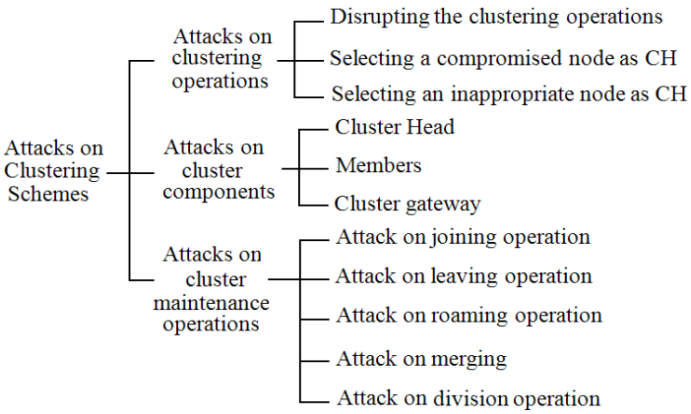


**Figure 2. Classification of Attacks on Clustering Operations**

In this section, we focus on general attributes and processing steps of general trust management schemes that are designed for MANET. However, before analyzing any trust based system, it is necessary to understand trust and reputation concepts. Generally, the following definitions have been presented for reputation in literature:

- The reputation of a node can be defined as its quality in terms of its behavior [16].
- Reputation is what is said or believed about a person's or thing's character or standing.

Although there are no clear consensuses on the definitions of trust, numerous definitions are presented in the literature:

- Trust is a subjective opinion in the reliability of other entities or functions.
- Trust can be defined as the expectation of one person about the actions of others [16].

Generally, trust describes a subjective relation between an entity and another entity (or group of entities), while reputation is what is generally said about an entity. Trust may be used to determine the reputation of an entity. In [16] Cho *et al.*, present a complete survey on trust management in MANET and specify that Trust is *dynamic, subjective, not necessarily transitive, asymmetric and context-dependent*. To use trust and reputation concepts in network, a reputation system should collect, distribute and aggregate feedbacks about nodes past behavior. Generally, a reputation system helps to decide to trust whom and it encourages trustworthy behavior and protects the network against attacks. To compute trust value, most of these systems utilize first hand information and second hand information. First hand information is the data that each node collects about its neighboring nodes and this can be done by eavesdropping broadcasted data in the wireless channel. The other information which trust system should achieve is the second hand information. These reports are sent by neighboring nodes and are not used unless the sender is trustworthy or the information is closer to what the receiver maintains [17]. Table 1 specifies the characteristics of first and second hand information.

**Table 1. Advantages and Disadvantages of First and Second Hand Information**

| First Hand Information | Second Hand Information |
|---|---|
| Fully reliable | Not reliable, Susceptible to lying attacks such as BM, BS and SP |
| No attack against it | Vulnerable to various external security attacks |
| Consume less energy than second hand information | Consume a lot of energy |
| Easily updated | Update is costly |
| Only compute the reputation of nodes which is in contact with them | Can compute the reputation of nodes that did not interact with them before |

The second hand information may be sent by malicious and normal nodes. Consequently malicious nodes can launch security attacks such as [18, 19, 38] *Bad Mouthing attack (BM), Ballot Staffing attack (BS and, Self-Promoting attacks (SP)*. These attacks can be controlled by careful considerations in trust value initialization and updated procedures. After gathering reputation information, the trust value is computed which reflects the degree of the trust between the trustor node and trustee node. Trust computation can be done in a centralized, distributed or hybrid approach. As Figure 3 shows, after trust computation, it should be decided that the trustworthiness of node is enough for a certain interaction or not, *i.e.*, it is trusted or not. This is usually done based on a threshold value which can be static and dynamic. If the trust value of a node is above the predefined threshold, then cooperation with this node is preferable. Otherwise it is not trusted and should be isolated from network. For example, its digital certificate or other security credentials should be revoked. After the revocation of compromised certificates and keys, this should be informed to the network users which can be done by CRL-based solutions or OCSP-based solutions such as ADOPT [20]. The possible threshold values which can be can be static and dynamic. It specifies that we can consider multiple thresholds for various tasks and operations. However, these trust values should not be remained intact for very long time and they must be updated somehow.

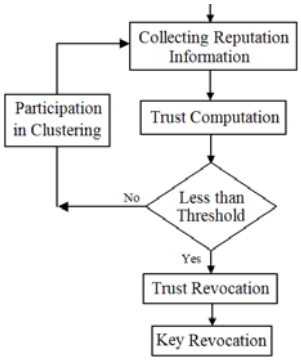


**Figure 3. Trust Evaluation Process**

### 2.1.1. Beta Reputation System

Most trust-based security schemes rely on Bayesian formulation as Beta reputation system for trust evolution. Beta reputation system is presented by Jøsang *et al.*, in [21]. In this scheme, prior probabilities of binary events can be represented as beta distributions which are composed of two parameters α and β. The beta distribution $f(p|\alpha, \beta)$ can be expressed by the gamma function Γ as:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}$$

$$0 \leq p \leq 1, \alpha > 0, \beta > 0$$

The probability expectation value of the beta distribution is given By $E(p)=\alpha/(\alpha+\beta)$

## 2.2. Key Management in MANET

The security of cryptographic solutions highly depends on the key management methods that they use. Generally, key management is defined as “the set of techniques and procedures supporting key establishment and maintenance of keying relationships between authorized parties”. In public key based security schemes, certificates are managed by two ways. In first case called web of trust, each node issue certificate for its trusted nodes and in second case called hierarchical trust, a certificate authority is used as a trusted third party for issuing and managing of certificates. The certificate authorities

were used by many security schemes in the centralized and distributed forms. Distributed Certificate Authority or DCA is realized through the distribution of the CA's private key to a number of shareholding DCA nodes and the public key of DCA will be known by all network's nodes and will be used to verify signatures of certificates issued by the DCA. When operations such as issuing or revoking certificates are required, a threshold of available shareholding DCA nodes should participate. In MANET, DCAs can be classified as partially or fully DCAs. In Partially implemented DCA or PDCA, tasks of the CA are distributed to a set of specialized nodes using secret sharing. But in Fully DCA, services of CA are distributed to all nodes. Table 2 shows the Properties of Partially DCA and Fully DCA.

**Table 2. Properties of Partially DCA and Fully DCA**

| | **Partially DCA** | **Fully DCA** |
|---|---|---|
| Client to DCA Communication | One-to-Many | One-to-Many |
| DCA to client | Many to One | Many to One |
| Security | Higher than FDCA | Low |
| Availability | Lower than FDCA | High |
| Mobility support | Low | High |
| Secret Update | Multicast | Broadcast |
| Scalability | High | Low |
| Special Nodes | Required | Not Required |

## 3. Proposed Schemes

This section briefly describes the trust-based clustering schemes which are presented in the literature. In [23] Elhdhili *et al.*, propose CASAN to elect trustworthy, stable and high-energy CHs. Their solution creates one hop members to minimize the overhead and take into account the trust level of a node, mobility, remaining energy and its distance to neighbors. For CHs selection, each node broadcasts a hello message with TTL 1 including its identification and mobility index. Then, each node with a trust level less than a threshold Trust min executes the non-trustworthy nodes procedure and others execute the trustworthy nodes procedure. In this process, each node computes its connectivity degree which is equal to the total number of distinct hello messages that it has received. Then broadcasts its metrics with TTL= 1 and uses received metric components of its neighbors to compute its weight as well as its neighbor's weights. If the node has the minimum weight compared to the weights in list, it proclaimed itself CH by sending a role message CHMSG to its one-hop neighbors. Otherwise, it launches a timer and waits for role messages from its neighbors with lower weights. If it receives at least one role message CHMSG, it attaches itself to the lowest weight CH and broadcasts a role message ORDINARYMSG to its one-hop neighbors to confirm its role as an ordinary node. Furthermore, this scheme elects nodes with low mobility as CH and to characterize the instantaneous nodal mobility, it uses a simple formula where each node i estimates its relative mobility index Mi by the following formula:

$$Mi = \sum_{j=1}^{n} WjD(i,j) = \sum_{j=1}^{n} \frac{\frac{1}{Mj}}{\sum_{i=1}^{K} \frac{1}{Mk}} D(i,j)$$

Where *D* is computed as the cumulative mean square distance to neighbors divided by the total number of neighbors.

In [24] Xu *et al.*, present a trust evaluation based clustering which CHs jointly perform the tasks of a certification authority and proactive secret sharing scheme is used to distribute the private network key to the CHs. In this solution, each cluster is first formed based on the trust values of the neighbor nodes. To create cluster, an ad hoc node evaluates its neighbor nodes' of neighbor nodes; each node chooses one node that has the

highest value as its trust guarantor. Then, the chosen node becomes the CH and the chooser becomes a member of the cluster, a node of the second highest trust value is chosen, in this way, a cluster is formed by the CH which has the highest trust value among the cluster members. After forming a cluster, the CH plays the role of trust guarantor. The CH evaluates and guarantees the trust of the cluster member nodes. When a member node requests it, CH issues the trust value certificate that contains the node's trust value. The member node uses the trust value certificate to show its trustworthiness to communicate with others.

The other trust-based clustering scheme is designed by Park *et al.*, in [33]. In this scheme each node evaluates the trust value of neighbor nodes and recommends one of neighbors that has the highest trust value as its trust guarantor. Then recommender node becomes a member of CH node which is one-hop away. When a node recommends some node as its CH, if the recommended node already became the member of other cluster, the recommender would have to recommend other nodes again. After that the one CH and its recommenders format a one hop range cluster. When nodes recommend a CH, they give a recommendation certificates called R-Certificate to the CH. These certificates are used to authenticate the CH. So, the CH which has many recommendation certificates considered as more trustable node in the ad hoc networks. In the recommendation certificate, the period is the term of validity of the certification. After the period, the CH has to request a new certification to the cluster member node. In which CH acts as a trust guarantor. It means that the member nodes which move to other place have to join the new cluster in the new place and maintain its trust in new places. Hence the new cluster in the new place refers the node's trust value by the previous CH for the trust evaluation.

VCA or Voting-Based Clustering Algorithm is another trust-based clustering scheme which is presented by Peng *et al.*, in [25]. It evaluates the stability of node through computing the neighbor change ratio and the residual battery power of mobile nodes. To elect CHs by using the voting mechanism, each node votes other nodes only if the node is the most trustful one among its neighbor nodes and the node's stability is better than itself. The transmission distance of vote is only one hop and the vote is not forwarded by other nodes, that is, each node only votes for its one-hop neighbor nodes. Each node in the network votes for its neighbor nodes according to the voting rules. By which we can conclude that the worse stability the node has, the more votes it gives; on the contrary, the better the stability it has, the more trustful it is, and thus with larger possibility it gets votes. Moreover, the fewer neighbors the fewer votes are obtained, even if it has better stability and is more trustful. Such nodes cannot act as CHs because they are often at the margin of the network. For Clustering the following procedure is executed:

- Each node computes its stability.
- Computes the trust of node with respect to its neighbors.
- Each node votes its neighbors according to the voting algorithm. Choose the largest $V(i)$ as the CH and if the number of votes is the same, choose the best stability as CH. If the number of votes and stability are the same, choose the smallest ID as CH.

Stability in this scheme is computed by the following formula:

$$NCR_i = \left| \frac{Si(t1) \cap Si(t2)}{Si(t1) \cup Si(t2)} \right|$$

Where $Si(t1), Si(t2)$ denote the number of neighbor nodes for node *i* at time *t1*, *t2*. The stability of each node is computed by the following equation: $S_i = \lambda_1 NCR_i + \lambda_2 P_i$ Where *Pi* is the residual battery power and $\lambda_1, \lambda_2$ are the weighting factors and $\lambda_1 + \lambda_2 = 1$. Table 3 compares the stability computation methods which have been used in trust-based clustering schemes.

| Table 3. Stability Computation in Trust-Based Clustering Schemes | | |
|---|---|---|
| **Ref#** | **Stability Computation** | **Stability Parameters** |
| 23 | $Mi = \sum_{j=1}^{n} WjD(i,j) = \sum_{j=1}^{n} \frac{\frac{1}{Mj}}{\sum_{i=1}^{K} \frac{1}{Mk}} D(i,j)$ | Cumulative mean square distance to neighbors divided by the total number of neighbors |
| 25 | $NCR_i = \lvert \frac{Si(t1) \cap Si(t2)}{Si(t1) \cup Si(t2)} \rvert$, $S_i = \lambda_1 NCR_i + \lambda_2 P_i$ | Number of neighbor nodes, Residual battery power |
| 26 | $MD_A = \frac{1}{N} \sum_{n-1}^{N} D_{A,n}$ $ST_A = MD_t - MD_{t-1}$ | Distances between node and all its neighbors |
| 36 | $RM_Y^{rel}(X) = 10log_{10} \frac{R_X P_{ynew} X \to Y}{R_X P_{yold} X \to Y}$ $RM_Y = var(RM_Y^{rel}(X_1), RM_Y^{rel}(X_2), \ldots, RM_Y^{rel}(X_m)$ | Based on received signal strength |

In [26] Kadri *et al.*, propose a secured weight-based clustering algorithm called SCA which includes a trust value defining how much any node is trusted by its neighborhood and used the certificate as node's identifier. SCA elects CH according to its weight computed by combining stability, battery and etc. It uses voting mechanism to elect the most trusted node. The CH election procedure is invoked whenever a neighborhood has no CH, or whenever one of the CHs isn't able to achieve its responsibilities. To create or maintain a clustering architecture, first the *Discovery stage* should be done. The purpose of this step is to get information about the neighborhood where the election procedure is invoked. Thus nodes desiring to be CH send *CH_ready* beacons within the radius of *D* hops. Each node when receiving this beacon estimates a trust value and sends it back to the asking node. After a discovery period, nodes having initiated this operation can derive from the received responses information such as *Degree, Stability, Trust value.* After the discovery stage, each node adds to the previous parameters the state of its *battery* and the *max value* then combines them with the corresponding *weight factors* and computes the *global weight*. Using the different received weights, nodes choose the node as CH which has the maximum weight. Then each elected CH need to discover each other to elaborate a virtual backbone to ensure inter-cluster services. Thus every new elected CH broadcast a discovery request over the network. CHs receiving this request register the certificate of the new CH and send him their certificate. In this scheme, stability is defined as the difference between two measures of average of distances between node A and all its neighbors (*MD)* at *t* and *t-1* $ST_A = MD_t - MD_{t-1}$ Where MD or mean distance is computed by this formula:

$$MD_A = \frac{1}{N} \sum_{n-1}^{N} D_{A,n}$$

In [27] Wang *et al.*, present a secure clustering scheme protocol that divides the MANET into several clusters and apply mesh topology structure. The CH is selected within the cluster, according to the number of the trust connections and the nodes which have trust connection with CH will be the core nodes. At first the cluster nodes set their trust values as 0. The cluster service group is made up of CH and core nodes. The CH and core nodes can join together to be the service group for the cluster, the service group is in charge of providing service for various requests from cluster members. The nodes which connect with the service group will be periphery nodes, they do nothing but forwarding the messages they have received. The messages between different clusters will be forwarded by the CHs, due to the existence of the session keys between the CHs, the messages can transmitted in the common channel.

In [28] Ferdous *et al.*, propose CH selection algorithm based on an efficient trust model. It aims to elect trustworthy stable CHs that can provide secure communication via

cooperative nodes. After deployment, the nodes broadcast their *ID* and TRUST value to their neighbors along with the REQ/REPLY flag. When the participating nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum neighbors from the trust interaction table is selected as the TA. Other nodes become members of the Cluster or local nodes. In [29] Chatterjee *et al.,* present a distributed trust based clustering framework. In this solution, the evidence of trustworthiness is captured from direct interactions and recommendations. After deployment each node sends "HELLO" beacon and try to find out how many nodes are deployed in its range. Each node receiving this beacon replies with his ID and public key. Each node getting this "REPLY" beacon increases the counter of its neighbor list, and stores node's ID and public key. Then an efficient secure distributed leader election algorithm SEC-LEAD is executed which can adapt itself to arbitrary topological changes. To reduce the computation overhead the CH selection mechanism only resumes if the existing CH runs off its battery or the CH has to move from its previous position. Secure Distributed Leader Election (SEC-LEAD) Algorithm consists of the following steps: In first step a node that wants to be CH broadcasts "START-ELECTION" message with its mobility, battery power value to all its one hop neighbors. Each node that gets this message within its broadcast range calculates the global weight of that candidate node using a global function:

$$G_w = w_1 * TV + w_2 * MV + w_3 * BP$$

Where w1, w2, w3 are different weights such that w1+w2+w3=1. If this value is greater than a predefined threshold, the node will vote for M by signing a Leader Certificate. After a certain time interval, the candidate node will count how many certificates it has already received. If this is greater than half of the neighbor nodes, it advertises itself as leader and broadcasts the leader message with the set of node-ids who has voted for it. If a node finds that its id is falsely included, it generates a warning message to all its neighbors.

**Table 4. Comparison Key Management Features in Trust-Based Clustering Schemes**

| Ref # | Authentication | Key Management | Stability |
|---|---|---|---|
| 24 | Certificate-based | a public and private key for every node, unique cluster key for every cluster, a unique pair of public/private key called head key for each CH | ---- |
| 26 | ---- | Public Key Infrastructure | ☑ |
| 27 | ☑ | Public Key Infrastructure, Nodes and clusters have their own keys, Session keys among the clusters | ☑ |
| 28 | Pairwise key | Public Key Infrastructure, a session key for inter cluster communication for each node and CH | ---- |
| 29 | Web-of-trust model | Public Key Infrastructure, Pair-wise key pre-distributed, CH nodes have to get access to the network key which is shared by CHs. Pair-wise secret key generated by pair of neighboring CHs. | ---- |

After certain time, neighbor nodes will sign a TrustCert for Leader, sends to it. Thus M becomes a Leader and the elector nodes who have signed the certificate become its member.

In [30] Wang *et al.,* present a novel self-clustering maximum flow algorithm to improve the search performance and scalability of MANETs with trust mechanism. In this solution, the trust relationship is formed by evaluating the level of trust using bayesian statistic analysis and clusters can be formed and maintained with only partial knowledge which makes it suitable for distributed autonomous MANETs. SCAR is another secure clustering algorithm that is designed by Yu *et al.,* in [31] and it takes into account a combined weight metric, including the reputation value, the node' degree and the relative mobility. In this solution, each node broadcasts Hello message to its neighbors

periodically and the weight information is carried in Hello message. When node receives Hello messages, updates the related nodes' reputation value. In addition, the node can update its degree and mobility, according to the number of Hello messages received and the transmission power. After receiving Hello message, the node gets its initial weight. Then the node sends its weight through the broadcasted Hello message. Compared with other nodes' weight, the node that has the highest weight is elected as CH. Table 4 shows the comparison key management features in trust-based clustering schemes.

### 3.1. Trust Management Issues

This section discusses about the trust management issues in trust-based clustering schemes and determines how node's trust is computed and what values for them are used? The computed trust value can be positive, negative or both of them. It can also be continuous or discrete but continuous values can represent uncertainty better than discrete variables. Determining the type and range of trust values is an important issue which has profound impact on the security and performance of trust management system.

**Table 5. Attacks on Second Hand Information**

| Trust Value | BM | BS | SP |
|---|---|---|---|
| Only Positive | ---- | ☑ | ☑ |
| Only Negative | ☑ | ---- | ---- |
| Negative and Positive | ☑ | ☑ | ☑ |

Table 5 shows various security attacks that can be launched against each type of trust value [18]. Although in [23] Elhdhili *et al.*, use trust and reputation factors but they do not specify how direct trust neighboring nodes are computed and how the indirect trust of network nodes collected and computed. In [27], the continuous real numbers between -1 and +1 are used in the qualification of trust value. The negative values indicate the degree of distrust, -1 represents complete distrust; the positive values indicate the degree of trust, +1 represents absolute trust. For a new adder, the trust value of it will be initialized as 0. Also, the trust value will be changed because of the increased recommendation trusts that are gained from a third node. In [28], the TRUST-VALUE is a continuous real number which range from 0.0 to 1.0, that zero specify the distrust and 1 determine the full trust.

In [33], the trust value of node is defined as a continuous value between 0.0 and 1.0. The value 0.0 means that node is totally distrusted and value 1.0 means that node is totally trusted. The trust value of node which does not have trust has to set the initial recommended trust value 1/2. But it can be changed according to the ad hoc networks. Scheme [36] uses the initially trusted or confident nodes which are honest. Each node manages a trust table and knows the identity and public key of other trust nodes and use trust metric as continuous value on the [0..1] interval. If a new node is added to the trust table by one or more confident nodes, all other confident nodes will be aware, because confident nodes update and exchange their trust tables. Each new node starts with TV = 0.1. In order to supervise the behaviors of nodes they propose hierarchical monitoring process. Each node with high trust value monitors its neighbor nodes with low trust value. In this trust model, the trust relationship is ensured by CAs between clusters. A CA can recommend node with certain trust level belonging its cluster to another CA. The trust value of a path depends on its trust chain which is represented by its certificate chain. The inter-cluster communication is based on the evaluation of certificate chain. In [37], direct trust between two nodes takes into account the individual experience of the past transaction. It is taken as 0.5 if there is no previous interaction between two nodes. If the first interaction be successful, the direct trust value will increase rapidly. Otherwise, it will decrease quickly. Also, in this scheme, the recommendation trust is calculated for unknown or unfamiliar nodes.

## 4. Conclusion

In this paper, we analyzed the state of art trust-based clustering algorithms which aim to detect and isolate the malicious and misbehavior nodes with low communication and processing overheads. Each security mechanism has its advantages and also overheads. Therefore, security mechanisms should be selected or designed considering their overheads and also the security requirements of environment. Although numerous secure clustering schemes have been presented for MANETs, there is a lack of solution to operate in both secure and hostile environments.

## References

[1] J. Y. Yu and P. H. J. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, **(2005)**.
[2] D. Wei and H. A. Chan, "Clustering Ad Hoc Networks: Schemes and Classifications", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, **(2006)**, pp. 920-926.
[3] S. Chinara and S. K. Rath, "A Survey on One-Hop Clustering Algorithms in Mobile Ad Hoc Networks", Journal of Network and Systems Management archive, vol. 17, no. 1-2, **(2009)** June, pp. 183-207.
[4] K. Erciyes, O. Dagdeviren, D. Cokuslu and D. Ozsoyellery, "Graph theoretic clustering algorithms in mobile ad hoc networks and wireless sensor networks", Applied and Computational Mathematics, vol. 6, no. 2, **(2007)**, pp. 162-180.
[5] R. C. Hincapie, B. A. Correa and L. Ospina, "Survey on Clustering Techniques for Mobile Ad Hoc Networks", **(2006)**.
[6] G. Kumar, K. K. Tripathi and N. Tyag, "Research Survey of Load Balancing Clusters in Wireless Ad hoc Network", International Journal of Electronics Engineering, **(2011)**, pp. 305-307.
[7] P. Rai and S. Singh, "A Survey of Clustering Techniques", International Journal of Computer Applications, vol. 7, no. 12, **(2010)** October.
[8] I. G.Shayeb, A. R. H. Hussein and A .B. Nasoura, "A Survey of Clustering Schemes for Mobile Ad-Hoc Network (MANET)", American Journal of Scientific Research, **(2011)**, pp. 135-151.
[9] R. Agarwal and M. Motwani, "Survey of clustering algorithms for MANET", International Journal on Computer Science and Engineering, vol. 1, no. 2, **(2009)**, pp. 98-104.
[10] Y. Zeng, J. Cao, S. Guo, K. Yang and L. Xie, "SWCA: A Secure Weighted Clustering Algorithm in Wireless Ad Hoc Networks", IEEE Wireless Communications and Networking Conference WCNC, **(2009)**.
[11] I. Nishimura, T. Nagase, Y. Takehana and Y. Yoshioka, "Secure Clustering for Building Certificate Management Nodes in Ad-Hoc Network", International Conference on Network-Based Information Systems, **(2011)**, pp. 685-689.
[12] H. Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks", Journal Wireless Personal Communications: An International Journal archive, vol. 56, no. 3, **(2011)** February.
[13] V. Sivaranjani and D. Rajalakshmi, "Secure Cluster Head Election for Intrusion Detection in MANET", Journal of Computer Applications, vol. 5, Issue EICA2012-4, **(2012)** February 10.
[14] P. Goyal, S. Batra and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, vol. 9, **(2010)** November, pp. 11-15.
[15] B. Wu, J. Chen, J. Wu and M. Cardei, "Wireless/Mobile Network Security", 2006 Springer, chapter 12.
[16] J. H. Cho, A. Swami and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, **(2011)**, pp. 562-583.
[17] J. Duan, Y. Qin, S. Zhang, T. Zheng and H. Zhang, "Issues of Trust Management for Mobile Wireless Sensor Networks", 7th International Conference on Wireless Communications, Networking and Mobile Computing, **(2011)**, pp. 1-4.
[18] H. Alzaid, "Secure Data Aggregation in Wireless Sensor Networks", Ph.D thesis, **(2011)**.
[19] J. Zhang, "A Survey on Trust Management for VANETs", International Conference on Advanced Information Networking and Applications, **(2011)**, pp. 105-112.
[20] K. Papapanagiotou, G. F. Marias and P. Georgiadis, "Revising Certificate Validation Standards for Mobile and Wireless Communications", Elsevier Computer Standards and Interfaces, Special Issue on Information and Communications Security, Privacy and Trust: Standards and Regulations, vol. 2008.
[21] A. Jøsang and R. Ismail, "The beta reputation system", 15th Bled Electronic Commerce Conference, **(2002)**.
[22] M. Masdari, S. Jabbehdari, M. Ahmadi, S. M. Hashemi, J. Bagherzadeh and A. Khadem-Zadeh, "A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks", 2011, EURASIP Journal on Wireless Communications and Networking.

[24] L. Xu, X. Wang and J. Shen, "Strategy and Simulation of Trust Cluster Based Key Management Protocol for Ad hoc Networks", Proceedings of 4th International Conference on Computer Science & Education, **(2009)**, pp. 269-274.
[25] S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad-Hoc Networks", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, **(2008)**, pp. 3-9.
[26] B. Kadari, A. Mhamed and M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 3, **(2007)** March, pp. 27-34.
[27] L. Wang and F. Gao, "A Secure Clustering Scheme Protocol for MANET", International Conference on Multimedia Information Networking and Security (MINES), **(2010)**, pp. 785-789.
[28] R. Ferdous, V. Muthukkumarasamy and E. Sithirasenan, "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks", International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, **(2011)**, pp. 589-596.
[29] P. Chatterjee, "Trust Based Clustering and secure routing Scheme for Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications, vol. 1, no. 2, **(2009)** July, pp. 84-97.
[30] W. Wang, G. Zeng, J. Yao, H. Wang and D. Tang, "Towards reliable self-clustering Mobile Ad Hoc Networks", Journal of Computers and Electrical Engineering, **(2011)**.
[31] Y. Yu and L. Zhang, "A Secure Clustering Algorithm in Mobile Ad Hoc Networks", IPCSIT, vol. 29, **(2012)**.
[32] V. Palanisamy and P. Annadurai, "Trust-based clustering for multicast key distribution scheme in ad hoc network (TBCMKDS)", Journal International Journal of Internet Protocol Technology, Issue vol. 6, no. 1-2, **(2011)**, pp. 46-64.
[33] C. Park, Y. Lee, H. Yoon, S. Jin and D. Chio, "Cluster based Trust Evaluation in Ad Hoc Networks", pp. 503-507.
[34] Y. Zhang, J. M. Ng and C. P. Low, "A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks", Journal Computer Communications archive, vol. 32, no. 1, **(2009)** January.
[35] Y. Zhang, J. M. Ng and C. P. Low, "A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks", Computer Communications, vol. 32, no. 1, **(2009)** January 23, pp. 189-202.
[36] A. Rachedi and A. Benslimane, "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks", 0-7695-2699-3/06/$20.00 (c) IEEE.
[37] V. G. Rani and M. Punithavelli, "Optimizing on Demand Weight -Based Clustering Using Trust Model for Mobile Ad Hoc Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 1, no. 4, **(2010)** December, pp. 81-91.
[38] F. G. Marmol and G. M. Perez, "Security threats scenarios in trust and reputation models for distributed systems", Journal of computers & security, **(2009)**, pp. 545-556.
[39] M. Masdari and J. Pashaei, "Distributed Certificate Management in Mobile Ad Hoc Networks", International Journal of Applied Information Systems, **(2012)** November 6.