Investigating Open Issues in Swarm Intelligence for Mitigating Security Threats in MANET

Pradeep Kumar K*, B.R. Prasad Babu**
* Dept of CSE, JNTUK, Kakinada (AP), India
** Dept. of CSE, SEA College of Engg & Technology Bangalore, India

Article Info

Article history:

Received Feb 22, 2015
Revised Jun 11, 2015
Accepted Jun 28, 2015

Keyword:

Ant colony optimization
Mobile adhoc network
Particle swarm optimization
Security
Swarm intelligence

ABSTRACT

The area of Mobile Adhoc Network (MANET) has being a demanded topic of research for more than a decade because of its attractive communication features associated with various issues. This paper primarily discusses on the security issues, which has been still unsolved after abundant research work. The paper basically stresses on the potential features of Swarm Intelligence (SI) and its associated techniques to mitigate the security issues. Majority of the previous researches based on SI has used Ant Colony Optimization (ACO) or Particle Swarm Optimization (PSO) extensively. Elaborated discussion on SI with respect to trust management, authentication, and attack models are made with support of some of the recent studies done in same area. The paper finally concludes by discussing the open issues and problem identification of the review.

Corresponding Author:

Pradeep Kumar K,
Dept of CSE, JNTUK, Kakinada (AP), India.
Email: pradeepkumarkrishnappa@gmail.com

1. INTRODUCTION

In Mobile Ad hoc Networks (MANET) [1], nodes are self-organized and use wireless links for communication between themselves. They dynamically form a temporary network without using any existing network infrastructure or centralized administration. These are often called infrastructure-less networking since the mobile nodes in the network dynamically establish routing paths between themselves. Examples are conference, battlefield, rescue scenarios, sensor networks placed in an area to monitor the environment, mesh networks for wireless Internet access etc. Routing solutions must address the nature of the network, and aim at minimizing control traffic, to preserve both bandwidth and energy at nodes. One of the major issues that affects the performance of an adhoc network is the way routing is implemented in a network. Routing algorithms used in conventional wired networks is impractical in adhoc networks due to its inability to adapt to the changing topology in a mobile environment. Generally, routing is the process of discovery, selecting, and maintaining paths from a source node to destination node deliver data packets. The goal of every routing algorithm is to direct traffic from sources to destinations, maximizing network performance whilst minimizing costs. This is a main challenge in MANET. Because the MANET possesses dynamic and random characteristics. Nodes move in an arbitrarily manner and at changing speed, often resulting in connectivity problems. The high mobility and the arbitrarily movement of nodes in MANET causes links between hosts to break frequently.

The self-organizing features of rapid deployment make MANET very attractive in military applications and earthquake prone regions where fixed infrastructure is not available. However, the dynamic nature of MANETs is easily vulnerable to attack. Misbehavior is one of the major problems in MANET implementation. It may seriously degrade the performance of the network. It can be categorized into selfish [2] and malicious misbehavior [3]. Selfish nodes intentionally misuse the MAC protocol rules to gain more access than well behaved nodes so that they can try to save their battery power without forwarding the relaying messages. In addition, they do not intend to involve themselves in the network damaging activities. In case of malicious misbehavior, malicious nodes intend to disrupt the normal network operation like denial of service attacks, timeout mechanism, choosing the small backoff value and jamming the wireless channel to prevent communication.

There exist several proposals that attempt to architect a secure routing protocol for mobile ad hoc network, in order to offer protection against the attacks. There are several solutions proposed by researcher they are either completely new stand-alone protocol or in some cases incorporation of security mechanism into existing one like DSDV and AODV [4]. Since routing is an essential function for ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of analysis is the examination of assumption and the requirements that each solution depend on. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment. In order to analyze exiting solution in structure way we have classified them into three categories; Solution based on Symmetric cryptography, solution based on Asymmetric cryptography and Hybrid solution. However, this classification is only indicative since a lot of solution can be classified into more than one category.

a. **Symmetric Cryptography Solutions**
   - Secure Efficient Ad hoc Distance Vector (SEAD) [5]
   - Secure Routing Protocol (SRP) [6]
   - Ariadne [7]

b. **Asymmetric Cryptography Solutions**
   - Authenticate routing for ad hoc network (ARAN) [8]
   - SAR [9]

c. **Hybrid Solutions**
   - Secure Ad hoc On-demand Distance Vector (SAODV) [10]

In the proposed review, we highlight a Swarm Intelligence approach in securing the communication system in MANET by reviewing the prior techniques applied. Section II discusses about the background of the study signifying the prior research attempts followed Problem description of the proposed study in Section III. Section IV discusses abouy the swarm intelligence approach while Section V discusses about the applicability of Trust management using Swarm Intelligence. Section VI briefs out the arrived problem statement of the study. Suggestion for research work in future direction is made as well followed by concluding remarks in Section VII.

2. BACKGROUND

Trust management schemes have been developed for specific purposes such as secure routing, authentication, intrusion detection, and access control (authorization). This paper summarizes existing trust management schemes by scheme name, methodology, attacks targeted, performance metrics used, and other notable characteristics of the proposed schemes. In existing system, it is to be noted that how the methodology explains the process that trust evidence is collected and performance metrics refers to the metrics used to evaluate the proposed trust management scheme. A narrative description of these schemes and an overview of some existing frameworks for trust evidence distribution and evaluation will be included in the journal version of this paper.

Some trust management schemes have been proposed in order to provide a general framework for trust evidence distribution or evaluation in MANETs. Jiang and Baras [11] proposed a trust distribution scheme called ABED (Ant-Based trust Evidence Distribution) based on the swarm intelligence paradigm, which is claimed to be highly distributed and adaptive to mobility. The swarm intelligence paradigm is widely used in dynamic optimization problems (e.g., traveling salesman problem, routing in communication networks) and is inspired from artificial ant colony techniques to solve combinatorial optimization problem. The key principle is called stigmergy, indirect communication through the environment. In ABED, nodes interact with each other through “agents” called “ants” that deposit information called “pheromones”; based on this the agents can identify an optimal path for accumulating trust evidence. However, no specific attacks were considered in [11]. Theodorakopoulos and Baras [12] proposed a trust evidence evaluation scheme for MANETs. The evaluation process is modeled as a path problem in a directed graph where nodes indicate entities and edges represent trust relations. The authors employ the theory of Semirings to show how two nodes can establish trust relationships without prior direct interactions. Their case study uses the GP web of trust to express an example trust model based on Semirings and shows that their proposed scheme is robust in the presence of attackers. However, their work assumes that trust is transitive. Further, trust and confidence values are represented as binary rather than as a continuous-valued variable. Even though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure. Recently Buckerche and Ren [13] proposed a distributed reputation evaluation prototype called GRE (Generalized Reputation Evaluation) to effectively prevent malicious nodes from entering the trusted community. However, no specific attack model was addressed. Further, transitivity, asymmetry, and subjectivity characteristics of trust concept were not specifically explained in building their trust model. Rajesh and Subramanian [14] also performed simulation study on wireless network using evolutionary algorithm. Similar study on wireless network towards communication protocol was also carried out by Hui [15]. The systems that are presented in this work are categorized primarily according to the adopted SI technique. The two main categories that accrue are: (a) IDS that make use of Ant Colony Optimization and (b) IDS that employ Particle Swarm Optimization. This section will present some of the recent work done using SI:

a. Recent Work in ACO

The basic principle of an ant routing algorithm is that ants deposit on the ground a hormone, the pheromone, while they roam looking for food. In [16], the authors have used a very simple and effective way of providing security against blackhole attack by introducing some modifications to ACO. Kumar and Kaur [17] have presented a work to identify a compromising path so that the reliable communication can be performed in MANET. Sharma et al. [18] proposed mechanism that protects the network through a self organized, fully distributed and localized procedure. The proposed work will reduce the network loss and improve the communication over the network. Indirani and Selvakumar [19] have examined performance of swarm based intrusion detection system under 3 mobility models by varying the speed and attackers in MANET using ACO.

b. Prior Work in PSO

PSO is a technique of optimizing the routes, results iterative and trying to growth towards the concluding result. Sandhya et al. [20] have optimized multipath route by selecting the best path using PSO. Key management scheme with MD5 hash encryption is proposed to improve the secure data communication. Jindal [21] has proposed a work to identify the broken link problem in a Mobile Network using PSO. Konak et al. [22] introduces a dynamic MANET management system to improve network connectivity by using controlled network nodes called agents using PSO. Dengiz et al. [23] introduced. A new approach to measuring connectivity using a maximum flow formulation. A particle swarm optimization (PSO) algorithm uses the maximum flow objective to choose optimal locations of the agents during each time step of network operation. Kavitha et al. [24] presented a framework on finding the optimum membership functions of a fuzzy system using particle swarm optimization (PSO) algorithm.

3. PROBLEM DESCRIPTION

Although there are various number of the issues in various problem domain in MANET using SI, hence in order to narrow down the focus of exploring open issues, we consider the following are the critical open issues after reviewing the literatures that has been introduced in the past:

a. Energy

Due to dynamic topology and affect of re-transmission, each mobile nodes are highly depleted of energy which comes from battery incorporated in the mobile device. Initially, it may be only though of raising quality of service issues like link breakage, node failure etc, but, carefully studying the fact will lead to discovery of the fact that when nodes are depleted of power, it leads to affect the communication between source and destination, in case the node is acting as intermediate node. The situation is somewhat similar to distributed denial of service attack to a large extent. Hence, for this reason, if there is any link disruption, it is hard to find out the real cause of it (whether it is caused by power depleted node or malicious node). None of the work discussed in previous sections has actually put forward any robust security scheme which is considers this fact.

b. Scalability

One of the yet unanswered issues in the area of MANET is to accomplish an efficient scalability of the network. An example of the work [25] [26] [27] [28] shows that the open issue is associated with the highest dimensionality of the mobile nodes that should be considered in mobile adhoc network at the time of evaluating security issues. Reviewing Section I, it can be seen that mobile adhoc network has lack of infrastructure with less computational capability and resource constraint. Maximization of number of nodes in MANET has substantial effect in the simulation result, which is still found not studied effectively with sufficient empirical proof with respect to assessing security problems. Moreover, if mobile nodes are found with increased mobility, it can lead to degradation of scalability.

c. Quality of Service (QoS)

The incorporated properties of the MANET system are the sole reason for quality of services too. Although various work like [28] [29], [30], etc has addresses the routing security, but it failed to address specifically more critical issues like channel capacity (packet delivery ratio, bandwidth, jitter, delay etc). It can be easily seen from all these above mentioned work that although the optimal security is established, but it has no positive effect on QoS parameters. Almost very less/limited focus on QoS issues are seen when game theory is applied.

4. SWARM INTELLIGENCE APPROACH

The term Swarm Intelligence (SI) was first introduced by Beni in the context of cellular robotics system [31]. Methodologies, techniques and algorithms that this research field embraces draw their inspiration from the behavior of insects, birds and fishes, and their unique ability to solve complex tasks in the form of swarms, although the same thing would seem impossible in individual level. Indeed, single ants, bees or even birds and fishes appear to have very limited intelligence as individuals, but when they socially interact with each other and with their environment they seem to be able to accomplish hard tasks such as finding the shortest path to a food source, organizing their nest, synchronize their movement and travel as a single coherent entity with high speed etc. This achievement becomes even more significant if it is taken into account that they accomplish such tasks without the presence of a centralized authority (e.g., the queen of the hive) dictating any of this behavior. Applications of this can be found in NP-hard optimizations problems such as the traveling salesman, the quadratic assignment, scheduling, vehicle routing etc.

The unique characteristics of SI make it ideal for this purpose. More specifically, SI techniques aim at solving complex problems by the employment of multiple but simple agents without the need of any form of supervision to exist. Every agent collaborates with others toward finding the optimal solution. This happens via direct or indirect communications (interactions) while the agents constantly roam in the search space. In this respect, agents can be used for several hard tasks like finding classification rules for misuse detection, discover clusters for anomaly detection, keep track of intruder trails etc. Indeed, these self-organizing and distributed attributes are highly appreciable by offering the means to break down a difficult IDS problem into multiple simple ones assigned to agents. This potentially makes the IDS autonomous, highly adaptive, parallel, self-organizing and cost efficient. In the literature the efficiency of such systems is usually evaluated against one of the existing benchmarks that specifically target IDS. The next section thoroughly surveys SI-based approaches used for securing communication system in MANET.

5. TRUST MANAGEMENT USING SI

The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. According to Eschenauer et al. [32], trust is defined as “a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities.” Trust has also been defined as the degree of belief about the behavior of other entities (or agents) [33], often with an emphasis on context [34]. Due to the unique characteristics of MANETs and the inherent unreliability of the wireless medium, the concept of trust in MANETs should be carefully defined. The main features of trust in MANETs are as follows [32] [33] [34] [35]:

A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.

- Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
- A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
- Trust is dynamic and not static.
- Trust is subjective.
- Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
- Trust is asymmetric and not necessarily reciprocal.

- Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

a. Trust Metrics for MANETs

Even though many trust management schemes have been proposed, no work clearly addresses what should be measured to evaluate trust. Liu et al. [36] defined trust in their model as reliability, timeliness, and integrity of message delivery to their intended next-hop. Also most trust-based protocols for secure routing calculate a trust value based on characteristics of well behaving nodes [36] [37] [38]. Trust measurement can be application-dependent and will be different based on the design goals of the proposed network. In this study, two types of trust based on trust relationships are discussed that require measurements of different aspects of trust.

- First, social trust refers to properties derived from social relationships. Examples of social networks are strong social relationships such as colleagues or relatives or loose social relationships such as school alumni or friends with common interests [39]. Social trust may include friendship, honesty, privacy, and social reputation/recommendation derived from direct or indirect interactions for "sociable" purpose. In MANETs, some metrics to measure these social trust properties can be frequency of communications, malign or benign behaviors (e.g., false accusation, impersonation), and quality of reputation.
- Second, QoS trust represents competence, dependability, reliability, successful experience, and reputation/recommendation on task performance forwarded from direct or indirect interactions with others. In designing network protocols, many prior works measured the trust value of a node based on performance metrics such as the node's energy or computational power, lifetime, packet delivery rate, or evaluations using reputation or recommendation from other nodes about task performance. The term QoS trust is used in this work to define trust evaluation mainly in terms of task performance capability.

b. Mitigating Attacks

Many trust management schemes are devised to detect misbehaving nodes, both selfish nodes and malicious nodes. Specific examples of network layer attacks are as follows [32] [33] [40] [41]:

- *Routing loop attack*: A malicious node may modify routing packets in such a way that the packets traverse a cycle, so that the packet does not reach the intended destination.
- *Wormhole attack*: A group of cooperating malicious nodes can pretend to connect two distant points in the network with a low-latency communication link called wormhole link, causing disruptions in normal traffic load and flow.
- *Black hole attack*: A malicious node, the so called black hole node, may respond always positively for route requests even without proper routing information. The black hole can drop all packets forwarded to it.
- *Gray-hole attack*: A malicious node may selectively drop packets, as a special case of black hole attack. Variations include the sinkhole attacker that selectively routes packets.
- *Denial-of-Service (DoS) attack*: A malicious node may block the normal use or management of communications facilities, for example, by causing excessive resource consumption.
- *False information or false recommendation*: A malicious node may collude and provide false recommendations/information to isolate good nodes while keeping more malicious nodes. This attack also called a black-mounting attack.
- *Incomplete information*: A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack. Distinguishing malicious behaviors from normal behaviors is difficult in MANETs.
- *Packet modification/insertion*: A malicious node may modify packets or insert malicious packets such as packets with incorrect routing information.
- *Newcomer attack*: A malicious node may remove their bad reputation/distrust by registering as a new user. The malicious node simply leaves the system and joins again for trust revocation, flushing out previous bad history and starting to accumulate new trust.
- *Sybil attack*: A malicious node can offer multiple identities to the network which can affect topology maintenance and fault tolerant schemes such as multi-path routing.
- *Blackmailing*: A malicious node can blackmail another node by falsely claiming that another node is malicious or misbehaving. This can generate significant amount of traffic and ultimately disrupt the functionality of the entire network.
- *Replay attacks*: A malicious node may replay earlier transmitted packets to the network. If the adversary replays route requests, old locations and routing information might make nodes unreachable.

- *Selective misbehaving attack*: This attack is derived from the subjective characteristic of the trust management framework. A malicious node may selectively provide or deny proper services.
- *On-off attack*: A malicious node may alternatively behave well and badly to stay undetected while disrupting services.
- *Conflicting behavior attack*: A malicious node may behave differently to nodes in different groups to make the opinions from different good groups conflicting, and ultimately lead to non-trusted relationships.

6. ARRIVED PROBLEM STATEMENT

From the justification laid down by the mitigation techniques using Swarm intelligence to generate optimal security in MANET, the problem identified from the review is that--"It is highly computationally challenging task to design a mathematic model to exhibit an extremely unpredictable malicious behavior of the malicious mobile nodes in multiples under diverse vulnerable security condition in MANET and thereby posing threat to design a decision making model for ensuring mitigating of attack events and deporting mechanism".

The above discussed problem statement has various rationale to justify the discussed point. One of the critical demerits of MANET system is its decentralization as well as its ongoing node mobility which consumes unwanted power and decision of routing protocol thereby posses a great challenging task. Due to this unwanted power drainage as well as limitation of channel capacity, there are some groups of nodes that may chose to reject forwarding or carrying any request from its neighborhood nodes due to its resource constraint. Such nodes are basically termed as Erroneous Nodes which rises due to technical issues of power or software/hardware problems. Existence of such nodes can be easily taken advantages by the malicious node which will always have certain harmful intention in order to paralyze the operational aspects of MANET system. However, there is a presence of other types of node in MANET which majorly imitates the behavior of Erroneous Node called as selfish node.

The characteristics adopted by selfish nodes targets to gain the benefit of network at the cost of other node resources opportunistically. Selfish nodes do not take part in packet forwarding and they are considered to behave very much rationally as they act opportunistically to gain network resources as advantages. Hence the presence of selfish node is potentially harmful as the similar behavior of the selfish node can be easily imitated by malicious node, which is the point of concern of many security aspects. As there is no presence of integrated digital certificate based node verification system among two mobile nodes in MANET, hence it becomes almost impossible task to identify the nodes to be regular, or selfish, or malicious.

A malicious node can easily furnish false information at the time of route discovery process by other regular nodes; they choose to participate even in node forwarding in the preliminary phases. This treacherous act of malicious mobile node will eventually gain the trust and belief system of the network where the malicious nodes seeks for an optimal opportunity to initiate a brutal attack on the network. It is to be noted that once the malicious node gains the trust, the more is the intensity of the attack potentially caused damaging various resources in MANET system. One of the most critical issues of such phenomenon is the identification of behavior of different types of nodes. Eventually, using cryptography or any other techniques will do stop and mitigate such attacks but cannot solve if the attacking strategy is changed by malicious nodes. Hence, working on intrusion detection system or detecting a malicious node will broaden the scope of study and optimal results on security on large scale MANET cannot be accomplished. Hence, the current research work chooses to simulate the decisions adopted by various types of nodes using game-theory that gives a better statistical probability of equilibrium stages.

7. CONCLUSION

It has been seen that majority of the above mentioned work is focused on introducing a strong security system that either addresses routing behavior or some other factors that directly influence node misbehavior using SI. However, almost majority of the work is found to have used cryptographic approach which always has some or other security loopholes when it comes to wireless networking. One of the interesting exploration was that even game theory has a valuable contribution in security of MANET [42] [43] where various approaches are used to mitigate attacks or any malicious activities in MANET. Hence, the future work could be on the direction of introducing a novel model based on game theory as well Swarm intelligence, which no one has ever attempted before. The notable contribution of the swarm intelligence can produce an efficient security system which can be further more enhanced by integrating with game theoretic concept of visualizing and discretizing mobile nodes. We strongly believe that such framework design can overcome various issues by eliciting various hidden traits of node behaviour in MANET in future.

REFERENCES

[1] J. Loo, et al., “Mobile Ad Hoc Networks: Current Status and Future Trends”, *CRC Press*, 2012, pp. 538.

[2] I. Aad, et al., “Denial of service resilience in ad hoc networks*”, In Proc. of ACM MobiCom,* 2004, pp. 202-215.

[3] A.A. Cardenas, et al., “Evolution of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments”, *IEEE/ACM Transactions on Networking (ToN)*, Vol. 17, No. 2, 2009, pp. 605-617.

[4] M. Akhlaq, et al., “Addressing Security Concerns of Data Exchange in AODV Protocol”, *World Academy of Science, Engineering and Technology*, 2006, pp. 29-33.

[5] YC Hu, et al., “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks”, *Elsevier, Adhoc Networks*, 2003, pp. 175-192.

[6] K. Sanzgiri, et al., “A Secure Routing Protocol for Ad Hoc Networks”, *IEEE International Conference on Network Protocols*, 2002, pp. 78-87.

[7] YC Hu, et al., “Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks”, *Springer, Wireless Networks*, 2005, pp. 21-38.

[8] K. Sanzgiri, et al., “Authenticated Routing for Ad hoc Networks”, *IEEE Journal on Selected Areas in Communications*, Vol. 23, Issue. 3, 2005, pp. 598-610.

[9] S. Yi, et al., “A Security-Aware Routing Protocol for Wireless AdHoc Networks”, *ACM Symposium on Mobile Adhoc Networking & Computing*, 2001.

[10] M.G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing”, *Mobile Computing and Communications Review*, Vol. 6, No. 3, 2002, pp. 106-107.

[11] T. Jiang and J.S. Baras, “Ant-based Adaptive Trust Evidence Distribution in MANET”, Proc. 2nd Int’l Conf. on *Mobile Distributed Computing Systems Workshops (MDC), Tokyo, Japan*, 2004, pp. 588-593.

[12] Theodorakopoulos and J.S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks”, *IEEE Journal on Selected Areas in Communications,* Vol. 24, No. 2, 2006, pp. 318-328.

[13] Boukerche and Y. Ren, “A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks”, *Proc. Int’l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada,* 2008, pp. 88-95.

[14] J. Rajesh, DV, Subramanian, “False Node Recovery Algorithm for a Wireless Sensor Network”, *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 2015, vol. 13, No. 2, pp. 379-386.

[15] L. Hiu, “A Novel QoS Routing Algorithm in Wireless Mesh Network”, *TELKOMNIKA*, 2013, vol. 11, NO. 3, pp. 1652-1664.

[16] K.S. Sowmya, et al., “Detection and Prevention of Blackhole Attack in MANET Using ACO”, *International Journal of Computer Science and Network Security*, 2012, Vol. 12, No. 5.

[17] D. Kumar, S. Kaur, “A Two Way ACO approach to Identify Next Secure Promising path in MANET”, *International Journal of Computer Networks and Wireless Communications (IJCNWC),* 2013, Vol. 3, No. 3, June 2013.

[18] P. Sharma, N. Sharma, R. Singh, “A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network”, *International Journal of Computer Applications,* (0975 – 8887) Vol. 41, No. 21, 2012.

[19] G. Indirani, K. Selvakumar, “Performance of Swarm based Intrusion Detection System Using Various Mobility Models in Manet”, *International Journal of Advanced Research in Computer Science and Software Engineering,* 2013, Vol. 3, Issue. 4.

[20] P. Sandhya, et al., “Ensuring data confidentiality in Manet by combining emphatic cryptography technique with PSO”, *Journal of Theoretical and Applied Information Technology*, 2013, Vol. 56 No. 1.

[21] J. Jindal, et al., “An Agent Based PSO for Route Reconstruction in Mobile Network”, *International Journal of Advanced Research in Computer Science and Software Engineering,* 2013, Vol. 3, Issue 6.

[22] A. Konak, et al., “Improving Network Connectivity in Ad Hoc Networks Using Particle Swarm Optimization and Agents”, *Wireless Network Design. Springer New York*, 2011, pp. 247-267.

[23] O. Dengiz, et al., “Connectivity management in mobile ad hoc networks using particle swarm optimization, Elsevier”, *Ad Hoc Networks*, Vol. 9, 2011, pp. 1312–1326.

[24] K. Kavitha, et al., “Particle Swarm Optimization For Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller”, *International Journal of Computer Trends and Technology (IJCTT),* 2013, Vol. 4, Issue 10.

[25] M. Dasgupta, et al., “Routing Misbehavior in Ad Hoc Network”, *International Journal of Computer Applications*, 2010, Vol. 1, No. 18.

[26] V. Kadam, et al., “An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in Manets”, *International Journal of Advances in Embedded Systems*, 2011, pp 04-06, Vol. 1, Issue 1.

[27] A.K. Gupta., et al., “Detecting and Dealing with Malicious Nodes Problem in MANET”, *International Journal of Scientific & Engineering Research*, 2013, Vol. 4, Issue 7.

[28] J. Sengathir, R. Manoharan, “Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs”, *I. J. Computer Network and Information Security,* Vol. 10, 2013, pp.1-10.

[29] J. Karjee, et al., “Tracing the Abnormal Behavior of Malicious Nodes in MANET”, *Wireless Communications, Networking and Mobile Computing, WiCOM '08. 4th International Conference*, 2008, pp. 1-7.

[30] M. Schutte, “Detecting Selfish and Malicious Nodes in MANETs”, *Seminar Paper*, 2006.

[31] G. Beni, et al., “Swarm intelligence in cellular robotics systems”, *In: Proceedings of NATO Advanced Workshop on Robots and Biological System*, 1989, pp. 703-712.

[32] L. Eschenauer, et al., “On Trust Establishment in Mobile Ad Hoc Networks,” Proc. 10th Int’l Security Protocols Workshop, Cambridge, U.K, Vol. 2845, pp. 47-66, 2002.

[33] L. Capra, “Toward a Human Trust Model for Mobile Ad-hoc Networks,” Proc. 2nd UK-UbiNet Workshop, Cambridge University, Cambridge, UK, 2004.

[34] W.J. Adams, et al., “Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration,” *Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW’05), West Point, NY*, 2005, pp. 317-324.

[35] Y.L. Sun, et al., “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks,” *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, 2006, pp. 305-317.

[36] R. Li, et al., “An Objective Trust Management Framework for Mobile Ad Hoc Networks”, *Proc. IEEE 65th Vehicular Technology Conf. (VTC’07)*, 2007, pp. 56-60.

[37] B.L. Zouridaki, et al., “Robust Cooperative Trust Establishment for MANETs”, *Proc. 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA*, 2006, pp. 23-34.

[38] A. Pirzada and C. McDonald, “Establishing Trust in Pure Ad Hoc Networks”, *Proc. 27th Australasian Computer Science Conf. (ACSC)*, Vol. 26, 2004, pp. 47-54.

[39] H. Yu, et al., “SybilGuard: Defending Against Sybil Attacks via Social Networks”, *IEEE/ACM Transactions on Networking*, Vol. 16, No. 3, 2008, pp. 576-589.

[40] K. Inkinen, “New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes,” *Seminar on Internetworking, Sjökulla, Finland*, spring 2004.

[41] C. Kardof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,*” Proc. 1st IEEE Int’l Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA,* 2003, pp. 113-117.

[42] P. Michiardi et al., “A Game Theoretical Approach to EvaluateCooperation Enforcement Mechanisms in Mobile Ad Hoc Networks," *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'03),* 2003.

[43] R. Mahajan, et al., “ExperiencesApplying Game Theory to System Design”, *Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems (PIN'04)*, 2004, pp. 183-190.

BIOGRAPHIES OF AUTHORS

Mr. Pradeep Kumar K. is currently working as Associate Professor in Govt. Sri Krishnarajendra Silver Jubilee Technological Institute, holding its responsibilities in Department of Computer Science & Engineering, Bangalore, Karnataka, India. He received the B.E. degree in computer science and engineering from Gulbarga University, Gulbaraga, India, in 2000, and the M.Tech, degree in computer science and engineering from the Visvesvaraya Technological University, Belgaum, in 2006 respectively. Currently pursuing research in the area of adhoc network security in Jawaharlal Nehru technical university, Kakinada, India. His research interests include network security, wireless communications and networking, game theory, swarm intelligence and cyber security. He is active member of the ieee communications society.

Dr. B.R. Prasad Babu is currently working as Professor and Head of Department in SEA College of Engg. & Technology, Bangalore. He received the B.E. degree in electrical engineering from Bangalore University, Bangalore, India, in 1983, and the M.E, degree in electrical engineering from the Mysore University, Mysore, in 1989 respectively. He obtained his Ph.D degree in computer science from the Mangalore University, Mangalore, India, in 2007. His research interests include Mobile adhoc networks, mobile communications, and wireless security. He published various research papers in leading international Journals, international and national conferences. Dr Prasad babu is a life member of ISTE, CSI and institution of engineers India. He is holding responsibilities of BOS and BOE member of the visvesvaraya technological university, Belgaum, India and Tumkur University, India.