A Bio-inspired Trusted Clustering for Mobile Pervasive Environment

Madhu Sharma Gaur and Bhaskar Pant

Abstract Pervasive systems are usually highly dynamic, heterogeneous, and resource-restricted where small and powerful dissimilar devices have to establish independent network unknown by the user. There is no fixed infrastructure and centralized access control. The set of connections relies on the convergence of wireless technologies, advanced electronics and the Internet to communicate seamlessly with other devices as tiny sensors. Trusted and Security-critical communication is the key concern in such decentralized and unpredictable environment. Bio-Inspired systems are increasing significant adaptation, reliability and strength in the dynamic and heterogeneous networks where information is ubiquitous. Some specific characteristics of swarms, like their lightweight, transient nature and indirect communication, make this adaptation more demanding. In this paper we explore bio-Inspired systems to look at the trust computation factors and opportunities in autonomic computing environments like mobile pervasive environment and evaluate their trustworthiness. We use standard clustering technique and propose a trust metric in which we observe the node behavior through various trust parameters. In winding up, we put our efforts to represent the cluster formation with honey bee mating to set up general vulnerabilities requirements for compromised node behavior to the system under exploration.

Keywords Clustering · Honey bee mating · Pervasive environment · Trust metric

M. S. Gaur (✉)
GEU, Dehradun, Uttarakhand, India
e-mail: madhu14nov@gmail.com

GL Bajaj Institute of Technology and Management, Greater Noida, India

B. Pant
Department of IT, GEU, Dehradun, Uttarakhand, India
e-mail: pantbhaskar2@gmail.com

M. Pant et al. (eds.), *Proceedings of the Third International Conference on Soft Computing for Problem Solving*, Advances in Intelligent Systems and Computing 259,
DOI: 10.1007/978-81-322-1768-8_49, © Springer India 2014

1 Introduction

The rapid growth of mobile computing has given rise to the information systems in which user can access the global network regardless of location or time. The words pervasive and ubiquitous mean “existing everywhere.” Pervasive computing devices are completely connected and constantly available. The vision of ubiquitous computing which Mark Weiser described in his 1991 paper [1] is based on the idea that future computers merge with their environment more and more until they become completely invisible for the user. Pervasive systems are usually highly dynamic, heterogeneous, and resource-restricted where small and powerful dissimilar devices have to establish independent network unknown by the user. There is no fixed infrastructure and centralized access control and set of connections relies on the convergence of wireless technologies, advanced electronics and the Internet to communicate seamlessly with other devices as tiny sensors and needs to be self adaptive and self-organizing.

Distributed wireless micro-sensor networks are an important component of the Pervasive computing that relies on the convergence of wireless technologies, advanced electronics and the Internet. A sensor node are location unaware and may not be equipped with GPS, can communicate directly only with other sensors that are within a small distance. However, in reality, sensor nodes are resource-restricted. Due to lack of fixed infrastructure, all the nodes have autonomous to make decisions based on the available information on the relying base station or mobile base station. All nodes are integrated into a wireless mobile pervasive Ad-Hoc network with multi-hop routing ability. Traditional security schemes cannot always be applied to such environments. Therefore, concepts like trust and reputation also applied to gain a certain level of security and confidence among inter-operating nodes. Up to the present, research on the trust management mechanisms of WSNs or MANETs have mainly focused on node’s trust evaluation to enhance the security and robustness where trust evaluation is the key concern to recognize malicious, selfish and compromised nodes which have been authenticated. In this paper we use standard clustering technique and propose a trust metric in which we observe the node behavior through various trust parameters. Clustering is a classic approach for achieving an energy efficient performance in sensor networks. Clustering provides locality of communication through organizing the number of nodes as clusters which saves energy and reduces network contention. In winding up, we put our efforts to represent the cluster formation with honey bee mating scheme, an energy efficient trusted cluster formation and head selection in pervasive mobile environment. Rest of the work is organized as II. Literature review, III proposed Trust Metric, IV A Bio-Inspired Cluster formation and finally conclusion and future scope.

2 Literature Review

We explore bio-Inspired systems to look at the trust computation factors and opportunities in autonomic computing environments like mobile pervasive ad-hoc networks and evaluate their trustworthiness Cho et al. [2], present a complete survey on trust management in MANET and specify that Trust is dynamic, subjective, not necessarily transitive, asymmetric and context-dependent. It can be defined as Direct and Indirect trust. LEACH (Low Energy Adaptive Clustering Hierarchy [3] is a cluster based protocol, which includes distributed cluster formation. For each cluster, a sensor node is selected as a cluster head. The cluster head applies aggregation functions to squeeze the data before transmission to the destination. PTM [4–6] a research sub-item of UBISEC (secure pervasive computing) supported by Europe IST FP6, which presents different models with revised D-S evidence theory and defines the inter-domain dynamic trust management in subjective area. The limitation of the PTM is that it acquires indirect trust value on average without taking the fuzziness, subjectivity and uncertainty into account. Lopez et al. [7] list the best practices that are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices. These references formulate an amazing summary, propose many profound viewpoints and show an additional insight on the trust evaluation field. In addition, other protocols [2, 8, 9] address trust management methods in self-organization networks from different views. A honey bee mating applications on clustering [10, 11] also inspire our proposed approach to present a bio inspired trusted clustering for pervasive environment.

3 Proposed Trust Metric

Our proposed trust metric based on social trust, QoS trust and reliability in terms of packet sent and received parameters to evaluate best possible aspects trustworthiness.

3.1 Trust Metric Parameters

The proposed trust metric key trust parameters are intimacy (for measuring nearness based on interaction experiences) and integrity (for measuring irregularity) to measure social trust derived from social networks. We choose energy (for measuring competence) and selfishness (for measuring uncooperativeness) to measure QoS trust derived from communication networks Table 1.

Here *intimacy evaluates* two node's neighbor nose's interaction experience. It follows the maturity model proposed in [8] where sensor nodes have more positive

Table 1 Trust Metric Parameters

$T_{xy}^{Intimacy}$	Intimacy for measuring nearness or closeness based on past experience
$T_{xy}^{Intigrity}$	Integrity for measuring irregularity or the honesty
T_{xy}^{Energy}	Energy for measuring competence or capability
$T_{xy}^{Selfishness}$	Selfishness for measuring uncooperativeness
$T_{X/Y}^{Mobility}$	Mobility to estimate the power consumption and residual energy of any node x
$T_{xy}^{\mathrm{Relaibility}}$	Reliability As total number of Packets sent by node x and received by node y

experiences. Assuming that a compromised node is malicious and untruthful, integrity component is taken that can efficiently identify whether a node is malicious or not. As a QoS trust metric energy is one of the most important components in the subjective resource-restricted networks. The unselfishness parameter specifies whether a node can cooperatively execute the intended procedure. In pervasive diverse devices or nodes are communicating seamlessly thus proposed approach can be applied in a heterogeneous network with immensely different energy levels and degrees of malicious or selfish behaviors. We apply this trust management approach to a clustered pervasive ad-hoc environment in which a sensor node may adjust its behavior dynamically according to its own operational state and environmental conditions. Here each node is more likely to become selfish in case of low energy level or it has many unselfish neighbor nodes around when it has more compromised neighbors around it.

$\boldsymbol{T_{xy}^{Intimacy}(t)}$ **:** It ranks the interaction experiences following the maturity model [8]. It is computed by the number of interactions between nodes x and y over the maximum number of interactions between node x and any neighbor node over the time period [0, t].

$\boldsymbol{T_{xy}^{Intigrity}(t)}$ **:** This refers to the confidence of node x that node y is truthful based on node x's direct observations toward node y. Node x calculate approximately T honesty, direct ij(t) by observing a count of suspicious untruthful experiences of node y which node x has observed during [0, t] using a set of anomaly detection rules such as a high inconsistency in the sensor reading or recommendation has been experienced, as well as interval, retransmission, repetition, and delay rules.

$\boldsymbol{T_{xy}^{Energy}(t)}$ **:** This refers to the belief of node x that node y still has adequate energy (representing competence) to perform its intended function. It may be measured by the percentage of node j's remaining energy. To calculate $T_{xy}^{Energy}(t)$, node x estimates node y's remaining energy by overhearing node y's packet transmission activities over the time period [0, t], utilizing an energy consumption model.

$\boldsymbol{T_{xy}^{Selfishness}(t)}$ **:** This parameter represents the degree of selflessness of node y as estimated by node x based on direct observations over [0, t].

Furthermore the selfish behavior of node y can be detected using eavesdrop and snooping techniques such as not honestly performing sensing and reporting functions, data forwarding summing that a compromised node must be uncooperative and thus selfish. If node x is not a 1-hop neighbor of node y, node x will use its former experience $Tc_{ij}(t - \Delta t)$ and recommendations for Selfishness it is also possible that a node doesn't route a packet from the other nodes or simply drops some packets to save their power or other energy. Thus such selfish nodes cannot have a high trust value because of the data delivery rate. By not providing packet forwarding for low trusted nodes, a network can encourage cooperation and reduce selfishness.

$T_{xy}^{\text{Relaibility}}$: The reliability of nodes can be evaluated in different ways, but, in general, it can be considered as the capability of nodes to respect a service agreement. This is a particular procedure that lies behind the identity certification or the encryption process. In the remaining part of this section, the word trust is used to identify the reliability of nodes. However, the protocol presented here can be easily extended to incorporate identity checking and trusting in the classic sense.

3.2 Algorithm Trust Evaluation (Calc-Trust)

Step 1: Collect data about a node (Xi to node n, where n is the total no of nodes in a cluster)

Step 2: Find the Trust threshold values associated to each behavior as described above

Step 3: Calculate trust value for each parameter [0.0–0.2]

Step 4: Aggregate all the trust value and find the mean corresponding threshold.

Step 5: Calculate the corresponding trust value using the formula.

3.3 Trust Calculation

The trust calculation is conducted, particularly between two neighbor nodes in a cluster. When a node X evaluates trust on another node Y at time t. We consider five trust components as described above like intimacy, integrity, energy, selfishness and reliability. The trust value that node X evaluates towards node Y at time t, Txy(t), is represented as a real number in the range of [0, 1] where 0 indicates distrust and 1 complete trust. Txy(t) is computed by

Table 2 Trust parameters and Cumulative Trust levels

Trust Parameters	Trust weight	Cumulative Trust Value	Level of trust
	0.0	0.0	Distrust
Intimacy	0.2	0.2	Very low trust
Integrity	0.2	0.4	Low trust
Energy	0.2	0.6	Partially Trusted
Selfishness	0.2	0.8	Highly trusted
Reliability	0.2	1.0	Fully Trusted

Table 3 Trust Value range of Trust Parameters

Trust Parameters	Trust Value Range of Parameter		
	0.0	**0.1**	**0.2**
Intimacy	No familiarity	Partial Intimacy	Fully intimate
Integrity	No Integrity	Partial Integrity	Full Integrity
Energy	No Energy Efficient	Partial Energy Efficient	Fully Energy Efficient
Selfishness	Unselfish	Partial Selfish	Fully selfish
Reliability	No reliable	Partial Reliable	Fully Reliable
	No Trust	Partial Trust	Full Trust

$$\mathrm{Txy(t)} = \mathrm{C1}{*}T_{xy}^{Intimacy} + \mathrm{C2} * T_{xy}^{Intigrity} + \mathrm{C3} * T_{xy}^{Energy} + \mathrm{C4}T_{xy}^{Selfishness} + \mathrm{C5}T_{xy}^{\mathrm{Relaibility}} \tag{1}$$

Where C1, C2, C3, C4, and C5 are costs associated with these five trust components with C1 + C2 + C3 + C4 + C5 = 1. Deciding the best values of C1, C2, C3, C4, and C5 to maximize system performance is a trust formation. We assume that each trust parameter is equally contributing in the process of Trust formation. Equation 1 can be rewritten

$$\begin{aligned}\mathrm{Txy(t)} = \; & 0.02\mathrm{C1} * T_{xy}^{Intimacy} + 0.2\mathrm{C2} * T_{xy}^{Intigrity} + 0.2\mathrm{C3} * T_{xy}^{Energy} \\ & + \; 0.2\mathrm{C4}T_{xy}^{Selfishness} + 0.2\mathrm{C5}T_{xy}^{\mathrm{Relaibility}}\end{aligned}$$

After collecting the information about nodes X and Y an Algorithm Compute-TRUST will be run to calculate the direct trust of node X about Y. Whenever the cluster head C-Hds inquires X's opinion about Y node, it will send the trust value. Assuming that each trust parameter have equal contribution in the final trust value $\mathrm{T}_{\mathrm{xy}}(\mathrm{t})$. On the basis of cumulative trust value after each parameter Calculated Suppose For example Tables 2, 3 and Fig. 1.

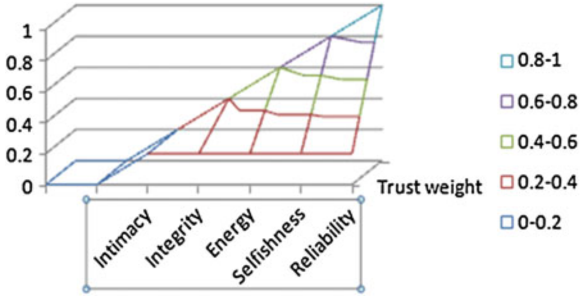

Fig. 1 Trust metric parameters

4 A Bio-inspired Trusted Cluster Formation

Clustering represents the different virtual groups of network sensor nodes which are physically neighboring and helps to organize the pervasive ad hoc networks hierarchically. Number of heuristic clustering algorithms has been presented in the literature and discuss about the latest developments in clustering like mobility-aware clustering, energy-efficient clustering, load-balancing clustering and combined-metrics-based clustering. In the mobile pervasive environments, nodes may differ from each other in terms of available resources and degree of mobility. Major resources are the communication, computation power and energy efficiency while the degree of mobility is the relative value to indicate dynamism of a node and average speed of the node. The magnitude of resources and mobility may differ continuously. As a whole, we assume that every node has different willingness value to be a volunteer set by its owner. A node that has abundant resources, a lower degree of mobility and a higher willingness value has a higher chance to be a volunteer. Any node can be a service provider (SP) as well as a service requestor (SR). The volunteers maintain a list of neighbor volunteers and a service directory for its range. We use a Service Discovery based on Volunteers for heterogeneous and uncertain pervasive computing environments. It provides a flexible and adaptable architecture appropriate for dynamic pervasive computing environments. We assume node-to-node connectivity in the network with common network/transport protocols such as TCP/IP. This approach uses a small subset of the nodes called collaborator that performs directory services to other nodes in the system. Here less mobile or nodes with high energy a nodes propose itself as a volunteer node in heterogeneous and uncertain (Fig. 2).

4.1 Trusted Clustering: Proposed Approach

The overall proposed approach is to dynamically organize the pervasive Sensor nodes clusters. Each cluster consists of one cluster head(C-Hd) node and an arbitrary number of clustered nodes(C-Nd). In each cluster, the C-Hd acts as a representative for its C-Nds and as nodes communicates their data over shorter

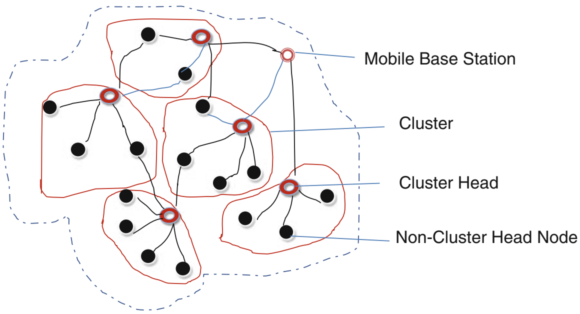

Fig. 2 Cluster

distances to their respective cluster heads. To save a substantial amount of energy, all the nodes that are not used continuously. The random selection of the cluster head node may obtain a poor clustering set of connections, and cluster head nodes may be redundant for some rounds of operation. Trust is calculated for a sensor node based on past interaction experiences given by neighbor nodes for assessing the reliability. It was also to measure the security of a node by evaluating whether a node is malicious or not. Trustworthy Architecture for such networks provides the trusted communication among the cluster nodes, based on trust and reputation formulations. Mobile pervasive Networks (MP-NETs) consist of a large number of relatively low powered mobile nodes, communicating in a network. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. Each group of nodes has one or more elected Cluster Head(s) C-Hds, where all Cluster heads are interconnected for forming a communication with limited energy sources for longer period of time. Misbehaving nodes and cluster heads can drain energy rapidly and reduce the total life span of the network. To ensure a secure and trusted communication cluster heads with trusted information becomes critical for the overall performance. The Cluster head(s) selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that can provide secure communication via cooperative selfish nodes.

4.2 Cluster Formation Algorithm

Clustering algorithm partitions a network into different clusters, creating a network hierarchy in the network. A particular node is elected in a cluster to manage the cluster information is known as the cluster head, and the other nodes are its members.

1. Any node can be volunteer to imitate the cluster formation.
2. Calculate the available Energy expressed by equation

$$\mathrm{En_y} = \frac{E_\mathrm{h} - E_c}{E_h} \tag{1}$$

where $\mathrm{E_c} = \mathrm{E_c} + \mathrm{E_{req}} + \square \geq 0$

3. Calculate the node stability or degree of mobility by the path planning.
4. Calculate the trust parameters as per pre-define threshold consider as a cluster member node.
5. The node with lowest mobility, high energy availability and highest trust as per above defined factors will be cluster head and will be responsible to provide service to each cluster node instead of each node itself.

Our Proposed cluster head selection algorithm is based on the analyzing the node misbehavior or compromising node detection based on the trust calculation. One of the essential operations in using clustering technique is to select cluster head among the nodes in the network and making a virtual group from the remaining nodes as a cluster around the cluster head node. In our proposed approach this done in a distributed manner, where nodes make autonomous decisions without any centralized control. The algorithm initially assumes that each sensor in the network becomes a cluster head with probability *p*. Each cluster head then advertises itself as a cluster head to the sensors within its radio range. This advertisement is forwarded to all sensors that are no more than k-hops away from the CH through controlled flooding.

Advantages and Limitations of Trusted Clustering: In our proposed approach, trust is calculated at two levels (a) trust at C-Hd level and (b) trust at clustered nodes CNs (Non-Cluster head node) level. Each C-Hd evaluates the cost of other C-Hds and C-Nds in its cluster while a CNs calculates other CNs in the same cluster in terms of trust value. The peer-to-peer trust costing is regularly updated based on direct or indirect observations. When two nodes are neighbors within a cluster, they evaluate each other based on direct observations. The C-Hd managers accomplish trust evaluation toward all C-Hds in the system. The selection of cluster head based on the most promising highest trust level or reader may refer protocols like HEED, LEACH [C-Leach] for a best possible solution. The description of these is outside the scope. If a C-Hds consumes more energy than a non-cluster head node is compromised, the more energy will be consumed to deal with attacks. Furthermore a selfish node consumes less energy than an unselfish node as its selfish behavior is reflected by stopping sensing functions and randomly dropping messages. Thus, the only secrecy of the system can be quickly sense and expel compromised nodes before a system failure. Considering the proposed approach in subjected area i.e. pervasive environment where the seamless communication relies on baseline technologies and may vary location to location and available infrastructure.

4.3 Honey Bee Mating for Trusted Cluster

Honey-bees mating is a swarm-based intelligence technique used in search optimization, inspired by the process of mating in real honey-bees. The behavior of honey-bees is the communication of their (1) Inherited potentiality. (2)

Environmental and physiological environments and (3) the social conditions of the colony. A typical honey-bee colony consists of a single egg laying long-lived queen (best bee), anywhere from zero to several thousand drones. The colony can be founded in two different ways as “self-governing origin” the colony starts with one or more reproductive females that build the nest, lay the eggs, and feed the larva’s. Later, division of labor takes place and the queen concentrates on egg laying and the workers in brood. A colony of bees is a large family of bees living in one bee-hive. A bee hive is like a big city with many “segments of the settlement”. The queen is the main vital member of the hive because she is the one that keeps the hive going by producing new queen and worker bees. With the help of approximately 18 males (drones), the queen bee will mate with multiple drones one time in her life over several days. The sperm from each drone is planted inside a pouch in her body. She uses the stored sperms to fertilize the eggs. Whether a honeybee will become a queen, a drone, or a worker, depends on whether the queen fertilizes an egg. Since she is the only bee in the colony that has fully developed ovaries, the queen is the only bee that can fertilize A queen bee may live up to 5 or 6 years, whereas worker bees and drones never live more than 6 months. Queens represent the main reproductive individuals which are specialized in eggs laying while Drones are the fathers of the colony. They are haploid and act to amplify their mothers’ genome without altering their genetic composition, except through mutation. Workers are specialized in brood care and sometimes lay eggs. Broods arise either from fertilized or unfertilized eggs. The mating process occurs during mating-flights far from the nest. A mating flight starts with a dance where the drones follow the queen and mate with her in the air. In a typical mating-flight, each queen mates with seven to twenty drones. In each mating, sperm reaches the spermatheca and accumulates there to form the genetic pool of the colony. In the mathematical representation, a drone is represented by a genotype and a genotype marker. Workers which are used to improve the brood’s genotype, represent a set of different heuristics. For example, at one-point of crossover heuristic, the crossover heuristic operator applies to the brood’s genotype with that of a randomly generated genotype where the crossover point is also selected at random. Each queen is characterized with a genotype, speed, energy, and a spermatheca with defined capacity. Spermatheca is defined as a repository of drones. In our proposes honey bee mating Queen is characterized by a fitness function based on trusted calculation based on above define parameters. The mapping of real honey bee and a pervasive network can be viewed in Table 4.

5 Conclusion and Future Work

In this paper, we proposed a bio-inspired trusted clustering for pervasive environment considering trustworthiness based on social and QoS trust parameters. In clustering technique If a C-Hds consumes more energy than a non-cluster head node the C-Hds is compromised, than more energy will be consumed to deal with

Table 4 Mapping of Natural Honey Bee Mating Pervasive Node's Mating

No#	Pervasive Node's (Bees) Mating	Natural Honey Bee Mating
1.	Nodes in pervasive adhoc Network	Bees in Hive
2.	Random node selection to broadcast as Cluster head with minimum mobility and maximum energy based on available base station or mobile base station information	Initial bee population
3.	Trust calculation to elect Cluster head with highest trust value (Queen)	Defining Fitness Function select Best Bee
4.	Drone Bee	Expected Cluster head list as per initial population Queen
5.	Working Bees	Heuristic Search Function
6.	Mating	Cross Over

trust calculation by evaluating peer nodes misbehavior. Furthermore a selfish node consumes less energy than an unselfish node as its selfish behavior is reflected by stopping sensing functions and randomly dropping messages. Thus, the only secrecy of the system can be quickly sense and expel compromised nodes before a system failure For Cluster formation we map subjective network with honey bee mating Honey-bees mating which a swarm-based intelligence technique. This technique is used in search optimization, inspired by the process of mating in real honey-bees to analyze the proposed approach in bee like network structure. As a further work simulation of proposed approach in dynamic scenario is ongoing. Identification of its application areas and implication is our future scope.

References

1. Weiser, M.: The computer for the 21st century. Sci. Am. **265**(3), 94–104 (1991)
2. Cho, H., Swami, A., Chen, I.R.: A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutor. **13**(4), 562–583 (2011)
3. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless mi-crosensor networks. IEEE Trans. Wireless Commun. **1**(4), 660–670 (2002)
4. Almenare, F., Marin, A., Campo, C., Garcia, R.C.: PTM: a pervasive trust management model for dynamic open environments. In: Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust, Boston, August 2004
5. Almenarez, F., Marin, A., Campo, C., Garcia, R.C.: TrustAC: trust-based access control for pervasive devices. In: Proceedings of the 2nd International Conference on Security in Pervasive Computing. pp. 225–238, Boppard, Germany, April 2005
6. Almenarez, F., Marin, A., Diaz, D., Sanchez, J.: Developing a model for trust management in pervasive devices. In: Proceedings of 4th IEEE Annual International Conference on Pervasive Computing and Communications. pp. 267–271, Pisa, Italy, March 2006
7. Lopez, J., Roman, R., Agudo, I., Fernandez, C.G.: Trust Management Systems for Wireless Sensor Networks: Best Practices. Comput. Commun. **33**, 1086–1093 (2010)
8. Bao, F., Chen, R., Chang, M., Cho, J.H.: Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manage. **9**(2), 169–183 (2012)

9. Hsieh, M.Y., Huang, Y.M., Chao, H.C.: adaptive security design with malicious node detection in cluster-based sensor net-works. Comput. Commun. **30**, 2385–2400 (2007)
10. Bozorg Haddad, O., Afshar, A., Mariño, M.A., Adams, B.J.: Honey-bee mating optimization (HBMO) algorithm for optimal reservoir operation. J. Franklin Inst. **344**, 452–462 (2007)
11. Fathian, M., Amiri, B., Maroosi, A.: Application with honey-bee mating optimization algorithm on clustering. Appl. Math. Comput. **190**, 1502–1513 (2007)
12. Li, J.L., Gu, L.Z., Yang, Y.X.: A new trust management model for P2P networks. J. Beijing Univ. Posts Telecommun. **32**, 71–74 (2009)
13. Marmol, F.G., Perez, G.M.: Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Comput. Stand. Interfaces **32**, 185–196 (2010)
14. Heinzelman, WR., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless micro-sensor net-works. In: Proceedings of 33rd Hawaii International Conference on System Sciences. pp. 1–10 (2000)
15. IEEE Commun. Surv. Tutor. 562–583 (2011)
16. M Wireless Conference (RAWCON'98), pp. 55–58 Aug 1998