Gaur and Pant *Hum. Cent. Comput. Inf. Sci.* (2015) 5:32
DOI 10.1186/s13673-015-0050-1

Human-centric Computing and Information Sciences
a SpringerOpen Journal

RESEARCH Open Access

Trusted and secure clustering in mobile pervasive environment

Madhu Sharma Gaur[1,2*] and Bhaskar Pant[3]

*Correspondence:
madhu14nov@gmail.com
[1] GEU, Dehradun, India
Full list of author information is available at the end of the article

Abstract

Pervasive computing has the potential to offer low-cost, high performance, and user centric solutions to exchange the information and communicate seamlessly in highly dynamic, heterogeneous environment. Here small and influential dissimilar devices or nodes have to set up independent network unknown by the user. Communicating devices are resource-restricted and equipped with micro or bio-sensors to acknowledge the signals where traditional security systems based on cryptography and encryption are not enough for promising level of security assurance. In this paper we explore trust and security challenges and appraise the opportunities in autonomous mobile pervasive ad-hoc networks to improve security. Trust management models in human-centric applications can enhance the security assurance. Many researchers proposed various trust models for different scenarios. Inspiring from such models we propose a trust computation metric based on node's impulsive behavior to become malicious node in dynamic scenario and breach the security. In winding up, we put our efforts to present energy efficient, secure and trusted clustering to enhance the security assurance and significant adaptation of trustworthy communication in user-centric m-healthcare applications where information is ubiquitous.

Keywords: Cluster, Pervasive environment, Security, Trust

Background

The vision of Pervasive computing has the potential to offer low-cost, high performance, and user centric solutions to exchange the information and communicate seamlessly in highly dynamic, heterogeneous environment where small and influential dissimilar devices or nodes have to set up independent network unknown by the user. Ubiquitous computing described by Mark Weiser [1] is based on the idea of future computers merge with their environment more and more until become completely invisible for the user. Such Environment has no fixed infrastructure and centralized access control. Communicating devices or nodes are resource-restricted and equipped with micro or bio-sensors to acknowledge the signals where traditional security systems based on cryptography and encryption are not enough for promising level of security assurance. In this paper we explore trust and security challenges and appraise the opportunities in autonomous mobile pervasive ad-hoc networks to improve security. Many researchers proposed various trust models for different scenarios. Inspiring from such models we propose a trust computation metric based on node's impulsive behavior to become malicious node

in dynamic scenario and breach the security. In winding up, we put our efforts to present energy-efficient, secure and trusted clustering to enhance the security assurance and significant adaptation of trustworthy communication in user-centric m-healthcare applications where information is ubiquitous. The set of connections relies on wireless technologies, advanced electronics and the Internet to communicate seamlessly. Such devices need to make decisions based on the available information on base or mobile base stations with multi-hop routing ability. Traditional security mechanisms with complex encryption and decryption with resource-restricted infrastructure is not enough to carry out security assurance in human centric applications like pervasive healthcare. In the literature many researchers proposed Trust, Reputation, Clustering and Bio-Inspired systems inspired from military applications such as battlefield surveillance. Many industrial and consumer applications are also using such networks for process monitoring, controlling, machine health monitoring, and so on.

Generally trust mechanism works in the three phases (1) node behavior monitoring, (2) trust measurement, and (3) insider attack detection. In this paper explore trust evaluation challenges, opportunities and Bio-Inspired systems in autonomic computing environment like mobile pervasive environment to enhance security assurance. Trust in human notion used in the highly dynamic and heterogeneous networks like mobile pervasive where information is ubiquitous tiny of micro-sensor nodes can estimate, update, and store the trustworthiness of other nodes based on the trust model. A lightweight trust computation approach based on the nodes' impulsive behavior monitoring with standard clustering proposed because it enables energy-saving. In winding up, Multi-objective functions for energy-efficiency evaluation discussed. Rest of the work is organized as II. literature review, III proposed trust computation model, IV trusted cluster formation, V security extension with pervasive m-healthcare case study as perspective applications, VI illustrate performance evaluation and comparison with traditional work and finally VII conclusion with future scope.

Literature review

Various trust management models used in heterogeneous networks like Wireless Sensor Network's, Mobile Ad-Hoc Networks (MANETs) for assessing the availability, reliability and security countermeasures through identifying compromised nodes. LEACH (low energy adaptive clustering hierarchy [2] is a cluster based protocol, that includes distributed cluster formation. The cluster head applies aggregation functions to squeeze the data before transmission to the destination. Based on past interaction experiences [3–6] proposed a reputation-based framework for data integrity in WSNs believed that it takes information collected by each node using a Watchdog mechanism to detect invalid data and uncooperative nodes. In [5, 7, 8] several trust and reputation management protocol discussed for WSNs by combining certificate-based and behavior-based trust evaluations. In trusted computing concept, devices always do as per expectation i.e. enforced both by hardware (trusted platform module-TPM) and encryption software. Trusted computing group (TCG) defined Mobile Trusted Module (MTM) [9, 10] to specify encryption/decryption, signature generation and sensitive data storage to deliver security functions. Security assurance cannot be randomly established between two nodes that are previously unknown to each other in a heterogeneous uncertain

scenario. Inspiring from the thought of about [Chang, Dillon, Hussain (2006)], "Trust is synonymous to Security". A distributed scheme combining continuous authentication and intrusion detection in high security MANETs [11], used to derive the ideal scheme of combining authentication and intrusion detection in MANET. Creation of a clusters and selection of a cluster-head may significantly contribute to the scalability, life span, and liveliness efficiency [2, 8, 12].

In [8] the authors have proposed a Time Constrained Bee's Mating approach (TCBMA) where cluster set up communication overhead reduced and elect the stand by node in advance for current cluster head that is able to withstand for many rounds in wireless sensor network. TRIUMF [13] is a trust routing protocol that describes the selfishness for MANET routing by packet sinking and in [14] trust estimated by security access points. In [15–18] research sub-item of UBISEC (secure pervasive computing) supported by Europe IST FP6, that presents different models with revised D-S evidence theory, to defines the inter-domain dynamic trust management based on the pervasive environment. The limitation of the PTM is that it acquires indirect trust value on average without taking the fuzzy, subjective and uncertainty into account. Lopez et al. [15].

Proposed trust computation

In the pervasive environment the mobile devices (bio-sensor nodes) connected in ad-hoc way for communication and needs to behave cooperatively. Though the security threats and attacks posed to specific node, mutual efforts in countering invasive behavior required. For an individual device limited intrusion detection mechanisms to their signal range while collaborative mechanisms are better alternatives for communicating suspicious activity and intrusions to other devices in the neighborhood. System model: in this paper we present trusted and secure cluster formation for micro-sensor devices called nodes to provide ubiquitous communication. The network may consists of low-cost, high performance, small and powerful dissimilar devices equipped with micro sensors capable of physiological dynamic behavior monitoring and multi-modal biometric continuous authentication in distributed environment. All these sensors rely on baseline infrastructure and controlled by a Base Station (BS). The BS acts as a gateway of the Wireless Sensor Network (WSN) to the outside world expected to have enough computational and communication capabilities. We assume that these devices equipped with multiple bio-sensors and continuous authentication. These devices are capable of collecting multiple biometrics and may behave maliciously.

Constraints in mobile pervasive environment

Pervasive communication is seamless communication in highly dynamic and heterogeneous with small and powerful dissimilar devices. All the efforts in progress serve to cut the limitations and obviate inherent challenges of mobile equipment that cause security concerns.

- *Limited resources* Although modern mobile devices reached a standard of 4 GHz plus multi-core processor units, hundreds gigabytes of storage capacity but still considered resource-restricted because of size, weight and power consumption limitations that should aggravate implementation of strong security mechanism on the device.

- *Highly dynamic and heterogeneous network* Topical mobile devices support different communication protocols as Bluetooth, Wireless Fidelity (Wi-Fi), 4G and etc. and quickly get connected within same or different overlapping networks which is always open to threats in an uncontrolled environment.
- *No fixed infrastructure* There is no fixed infrastructure and centralized access control. Set of connections relies on underlying and make decisions based on the available information on the relying base station or mobile base station with multi-hop routing ability.
- *Connection swings with limited bandwidth* Due to mobility distance to base stations and access points affects the signal quality and low down that may also lead to security threats.
- *Limited user interaction* Pervasive computing provides user-centric solutions but due to low size display, lack of fast and responsive user interfaces may cause security breaches by making users ignore protections as screen locks.
- *Dependence on battery power back-up* Computational usage and performance depend battery life and recharges should yield physical threats to device.
- *Lack of mechanisms of identity control* In the subjective environment devices spontaneously connected but lack of central administration arise big challenges in the identity management of non-operator-controlled.
- *Co-operation* Algorithms in pervasive environment assumed self-adaptive, self-organizing and co-operative.

Trust and security challenges

Pervasive computing offers make it inclined to more vulnerabilities and disclosures concluding an extra responsibility to the security subsystem and rely following challenges

- *Computing environment* Subjective environment is intangible to conventional computing, resource limitation and site constraints. Thus traditional methods concentrating solely on digital security are insufficient.
- *Privacy issues* Due to physical outreach of pervasive communication privacy and confidence track is complex.
- *Trusted security* Trust is an association between two entities such that one entity credits other trusted entity and also is a representation of being reliable, secure and trustworthy in any interaction with the node. A trusted security task will enhance the acceptance and provides autonomous decision making.
- *Social issues* Social implication regarding the adoption and acceptance such environment in day today life impose strong security models with privacy and trust.

Malicious node detection

Node's impulsive behavior leads malicious behavior. Dynamically malicious detection based on immoral snooping of the communicating channels. In general snooping leverages two inherent properties in mobile ad-hoc protocols where first one is that each node maintains a neighbor list containing the addresses of those nodes with which it is in immediate proximity or on the path from a source to a destination. The second property, as in 802.11 [19] and MACAW [20] link layer protocols, is that a node is able

to hear negotiation of its neighbors. Reasonably the malicious behavior can be due a compromised or selfish node, user or code. Viewing pervasiveness and dynamic network topology with the support of self-configuration, we use peer reputations to dynamically detect and deny resources for trust evolution using standard clustering concept based on prior encounters to develop trust and security. Using context information and notions of neighborhoods a node need only to store relevant information. Furthermore, if any malicious or compromised behavior is credited to any known entity, the fact can be reported back in the community where that entity is known to be a repeated company. As without assurances of security and trustworthiness of retrieved data, the utility and effectiveness is always doubtful. To address challenges of security assurance and trusted communication, secure routing, peer discovery, data management metrics to evaluate peer-provided information must be available.

Scenarios for monitoring dynamic behavior of a node We consider following scenario in the monitoring intrusive/malicious behavior dynamically to design security aware framework:

- *Node's impulsive behavior* With high mobility and self-motivated infrastructure, new permissible routes available that are difficult to detect during the learning phase and a node may route insensitively as per available resources.
- *Impulsive node behavior cause malicious* Spontaneous node insensitive behavior the node starts misbehaving cooperatively or being compromised and start promoting the permissible routes that may not be available.
- *Compromised behavior direct towards apprehension* Routes that are part of that node about to become available as genuine routes and accordingly node behavior may clue unusual threatening.
- *New compromised behavior* Routes that are never observed in the learning phase become part of non-self with variable and insincere route vulnerabilities.

In this way we can dynamically detect malicious node in two levels; one by route snooping to detect impulsive behavior throughout the communication channels with in cluster and other is by trust computation described ahead based on QoS and Social behavior of communicating nodes.

Trust computation parameters

We assume that each node maintains a table to keep its social and QoS trust factors as per their dynamic behavior between two communicating node as X and Y over time t that will autonomously updated when it interact with other node on demand or expiry to save resources. We consider following trust parameters for evaluating the node information Table 1.

Trust calculation is consists of two processes where first evaluate the communicating node table credentials about trust factors and second calculates the mean of trust value based on each parameter as per predefined threshold.

$T_{xy}^{Intimacy}$(t): it measures the interaction experiences following the maturity model [21]. It is computed by finding the ratio of positive number of interactions between nodes x and y over the maximum number of interactions over the time period [0, t] as

Table 1 Trust calculation factors

Node's Behavior	Trust between node x and y over time t	Meaning (measures between two nodes X and Y)
Intimacy	$T_{xy}^{Intimacy}(t)$	Interaction experiences
Integrity	$T_{xy}^{Intigrity}(t)$	Confidence
Mobility	$T_{xy}^{mobility}(t)$	Battery life and mobility mis-behavior
Selfishness	$T_{xy}^{selfishness}(t)$	Degree of selflessness
Reliability	$T_{xy}^{Reliability}(t)$	Packets being lost, inserted and multiplied

$$T_{xy}^{Intimacy}(t) = I_x = (P_x/T_x) \tag{1}$$

where I_x is the interaction ratio considering only positive Interaction P_x over total no of Interaction T_x through node x.

$T_{xy}^{Intigrity}(t)$: 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) by observing a count of suspicious untruthful experiences of node y that 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 as in [2].

If the count exceeds a system-defined threshold, node y is considered totally dishonest at time *t*, i.e., $(t) = 0$. Otherwise, (t) is computed by 1 minus the ratio of the count to the threshold. It can be measured as recommending service to define how trust value recommended by the recommending service and is given by:

$$T_{xy}^{Intigrity}(t) = c \times \gamma \times S \tag{2}$$

where c is normalized interaction value, γ is over time t experience and S is security level of recommending Service Interface.

$T_{xy}^{mobility}(t)$: we assume node mobility as a significant parameter to estimate the battery life where average distance between nodes required with limited energy provided. Hence it is desired to balance the motion characteristics for attaining the overall coverage and better network life. Thus average movement can measured by two factors, first the mobility incidences of the sensor nodes in a given time (t) bounded by a battery life threshold where high mobility with limited battery life will be punished that makes it highly unaffordable to achieve cooperative and second Uncertainty measures misbehavior of nodes during failure to stabilize themselves in competitive forces where nodes are penalized for irregular haziness. Thus the node mobility mis-behavior impact can be measured for given time t as

$$T_{xy}^{mobility}(t) = ((1 - M_x(E, D)) + (1 - P_x(t)))/2 \tag{3}$$

where $P_x(t)$ is the x sensor node's penalty measure for visit the similar position for t times ($0 \leq Px(t) \leq 1$), and $M_x()$ is the node x punishment credentials with $0 \leq M_x(E, D) \leq 1$.

Here E energy or battery status represented in quantized steps and D is the estimated distance traveled by the node mobility which is estimated on the basis of energy-based localization with multiple energy reading at different known multi hop sensor locations.

$T_{xy}^{selfishness}$(t): it 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 eavesdropping and snooping techniques, data forwarding summing that a compromised node must be uncooperative. By the monitoring impulsive behavior of mobile nodes in subjected area we observe malicious and selfish behavior of nodes where a selfish node needs to use network resources and saves own resources "drop any forwarded packet form other nodes and don't want to be a member in any new routes" while malicious node needs: to be a member in all new routes and mount a denial of service attack by dropping the packets it receives. We will allow some degree of selfishness for nodes to save their resources where nodes behave differently based on their energy levels. Assuming that if a node has full energy level as per threshold the node should behaves properly but if energy level lowers than the threshold it will use its energy for transmissions of its own packets. If multi-hop node x neighbor of node y, node x will use its past experience and recommendations for selfishness. 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, such autonomously encourages cooperation and decline selfishness.

$$T_{xy}^{selfishness}(t) = (F_x - D_x)/F_x \tag{4}$$

where F_x are the total number packets forwarded by node x and D_x is the number of packed dropped over a time.

$T_{xy}^{Reliability}$: the reliability of nodes may be evaluated in different ways, but, in general, it may be defined 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 also that may be evaluated in different ways, but, in general, it can be considered as the capability of nodes to respect a service agreement. Trust based reliability over a time t can be computed as probability of packets being lost, inserted and multiplied as

$$T_{xy}^{Reliability}(t) = (|Sp - Rp|)/Sp \tag{5}$$

where Sp = Total no. of packets sent by Y to X and Rp = Total no. of packets received by Y sent from X.

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 assume 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:

$$Txy(t) = C1 \times T_{xy}^{Intimacy} + C2 \times T_{xy}^{Intigrity} + C3 \times T_{xy}^{Energy} + C4 T_{xy}^{selfishness} + C5 T_{xy}^{Reliability} \tag{6}$$

where C1, C2, C3, C4 and C5 are costs associated with these five trust factors with equal threshold of 0.2 for each factor and 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.

Algorithm trust evaluation (Compute-TRUST)

Step 1 Analyze node X and Y data tables to calculate the direct trust based on interaction
Step 2 Calculate trust value for each parameter
Step 3 Find the each parameter corresponding trust value as per pre-defined threshold [0.0–0.2]
Step 4 Calculate the final Trust value TXY value over a specified time on demand based on the dynamic behavior of node
Step 5 Aggregate the trust value as per weighted cost as per using the formula

We assume that each trust factor as defined in Table 2, is equally contributing in the process of Trust calculation for ranking the trust level as depicted in Fig. 1. 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.

Trusted cluster formation

Security-critical communication is core stone in decentralized, highly dynamic and unpredictable mobile pervasive environment where small, effective and resource-restricted devices are communicating seamlessly. Clustering is a standard energy efficient technique used in sensor networks to provide locality of communication through organizing the several nodes in different virtual groups known as clusters that saves energy and reduces network contention. Here sensor nodes are physically neighboring and helps to organize the pervasive ad hoc networks hierarchically. An essential operation with clustering technique is to select cluster head shown in Fig. 2. The base station or mobile base stations are satellite based setups or machines capable of analyzing the data collected from the cluster heads and displaying a global view of actions being monitored.

Inspired by Multi-objective optimization [22, 23], where multiple optimal solutions using multiple fitness functions used at same time to find optimal solution. Underlying

Table 2 Trust parameters and cumulative trust levels

Trust parameters	Cumulative trust value	Ranking of trust
	0.0	Distrust
Intimacy	0.2	Very low trust
Integrity	0.4	Low trust
Mobility	0.6	Partially trusted
Selfishness	0.8	Highly trusted
Reliability	1.0	Fully trusted

details description of the Multi-objective underlying concepts is avoided just focus directly to aimed work. Here fitness function is a function used to measures the optimality of a solution in evolutionary algorithm. In multi-objective optimization multiple optimal solutions using more than one objective function at same time.

Thus inspired by a multi-objective optimization, we use three objective functions F1(), F2() and F3() Our cluster head selection algorithm is based on proposed trust calculation metric as defined above in Eq. (6). The algorithm initially assumes that each sensor in the network may become a cluster head with probability 1 or 0 where nodes make autonomous decisions without any centralized control to measure the trustworthiness of the node, life time and extended security.

The fitness function In the proposed work, the fitness is evaluated based on three objective functions F1(.), F2(.) and F3(.) where F1(.) computes the trustworthiness T_{xy} Eq. (6) of the node, F2(.) is used to estimate the remaining lifetime or residual energy for to elect the cluster head with a probability p which is proportional to the residual energy of the node. Thus a sensor node with higher remaining lifetime has higher possibility to become head. Suppose Lt is the predicted life time of the system before set up the sensors and T_c be the time consumed to set up of the n sensor nodes as cluster, then total residual energy Et_{resi} of all sensor nodes can be estimated as

$$Et_{resi} = \frac{nE_{ini}(L_t - T_c)}{L_t} \tag{7}$$

where E_{ini} is the initial energy of each node and n is the total number of nodes.

Further the probability p proportional to the residual energy can be defined to the as if Lt number of candidates is m % of the total number of nodes with remaining energy E_r then

$$P = n \times \frac{E_r}{Et_{resi}} \times \frac{m}{100} \tag{8}$$

The cluster radius of node varies with residual energy of node and the distance between nodes to the base station. Thus, the node closer it is to base station, the lower is the residual energy and the smaller is the radius of the clusters.

Saving resource usage We aim trust computation in highly dynamic and heterogeneous where the hardware equipment have limited processors and memories. Unlike in [12] where a mesh-like approach used to calculate trust by each node in the network has needs to update trust table of all nodes in the network and resources are wasted on updating trust values if node may expire before being used. By using clustering we put our efforts to minimize the resource usage resources as much as possible. Because of pervasiveness, each node need to be self-organized, independent and a cluster head C-Hd node will store trust values of nodes communicating with it only, to reduce the memory usage by ignoring trust calculation along with nodes that had left the neighborhood or remain dead in the network.

Finally F3 (.) measures node security, we aim trust computation in highly dynamic and heterogeneous where the hardware equipment have limited processors and memories. Fitness with cluster formation to enable security on nodes based insider attacks and threats involved in data integrity for secure communication. Sink node maintains the log

of all the ill-formed packets received by following specific path. If any path from C-Hd to sink or vice versa carries abnormal and retried packets, they are penalized for allowing authentication on routers (ICR) and encryption on cluster-heads. Additional penalty is also awarded if the authentication is enabled un-proportional to threat level quantized to M levels. The system can react proportionally to the perceived threat and the energy efficient enablement of security attributes that are measured against energy or battery lifetime threshold levels and rate of battery usage based on data communication, average number of connecting nodes, and mobility.

$$\mathrm{F3}() = 1 - \frac{1}{2P}\sum_{i=1}^{P}\left(\left|\frac{\theta_i}{M} - \frac{\lambda_1 S_i + \lambda_2}{N}\right| + \sum_{n=1}^{N}\frac{f(Q,\varphi)}{N}\right) \tag{9}$$

where λ1 and λ2 = 1 with λ2 penalized expense due to encryption of the Initial node (Xi), P is the total number of possible paths and θ_i is the threat of evaluated path calculated by sink, S_i is the number of nodes (ICR(s) and C-Hd) that are enabled for authentication and encryption in route i, N is the total number of nodes (ICR(s) and C-Hd) in route i, In i = 1 if node n in route i is enabled for authentication, and function f() is penalty for enabling admission control on node i on route j that has energy level at Q and rate of battery usage at Ã.

Security extension pervasive m-healthcare: a case study

Security settings competes with node mobility and assigned corresponding fitness factors that may not be optimal for securing the packets due to battery conditions that activates until all objectives reach an acceptable convergence for cluster head node selection, path selection, energy and mobility estimation are the dynamic processes that repeats over the subjective search space. Mobile pervasive cluster communication initiated by the Base Station (BS) and cluster-heads and needs to be secured. Messages in this kind of communication include key exchanges, misbehaving node removal. Almost of the existing authentication protocols require a trusted third party that generates secret keys for the communicating parties for the we propose the an arbitrary Authentication scheme with low-energy and resource requirements as every node has assigned an uncommon Id and a security code. All the Ids and security code pairs are stored at the base station and while any kind of communication from the node through the cluster heads periodically verify the sender as

1. The cluster head generates a random number receives while receiving communication request as R, as $0 \leq R \leq 1$.
2. If $R \leq p$ (predefined probability) that a cluster head requests the sender for its security code.

The cluster head sends the pair secure code id to the base station for verification. This requires identifying compromised energy available and preventing listening by penalized routers as extended security which deals with authentication and integrity of a message needs to be able to be unambiguously ensure that the communication so far done between source and cluster head was not altered in transit in order to mask the current environment. The imposed security elements reconcile through the trusted behavior and

energy efficient authentication. First initiator is a cluster-head and security setting fight with cluster head selections with their behavior. Nodes are assigned functions or locations based on the corresponding fitness factors which may not be optimal due to their compromising behavior, energy level for security assurance. Similar to node selection, route selection, and mobility estimation, size of cluster and area can be also considered over the system life-time to make it optimal solution in the subjective search space.

Performance evaluation and comparison with traditional work

Pervasive ad-hoc sensor network one of the largely acknowledged technology for the twenty-first century for human-centric application by creating smart space in home, office, on the way and life threatening industrial application like mining. For better livings IT enabled services where deployment of micro or bio sensors carried out in an ad-hoc manner without cautious sensing electronics assessment of environment conditions. Telecommunication industry has also recognized the forte of pervasive applications. Similarly, we would like to put our efforts in the formation of a trusted cluster of m-healthcare stake holders that can be an instrument for immediate pervasive healthcare anywhere any time by sharing vital parameters from remote locations. Our contribution is in the way of realization of pervasiveness for ideal healthy community by providing remote monitoring of critical patients and aged people staying alone at home, workers struggling for their living in mines by remotely empowering the healthcare centers situated at distant locations with limited facilities in Indian scenario.

Experiment setup To evaluate performance of proposed approach, we experiment and simulated the dynamically malicious node detection with trust computation. All the experiments show that our design principle can be applied to a wide spectrum of algorithms to achieve comparable performance with much better robustness. We simulate a Pervasive Ad hoc network with 500 m $\times$ 500 m field with different pervasive devices or nodes 10–50 with random distribution. The sensors have radio range of 40 m. A Base Station is at the top of the network to allow communication from the all the sensor nodes. The Routing Protocol AODV Data Rate 80 per 0.005 s Packet Size 64 bytes simulation time 20 s using OPNet and SensorSimulator to show the results with different number of nodes in the network. As the number of nodes in the network increases,

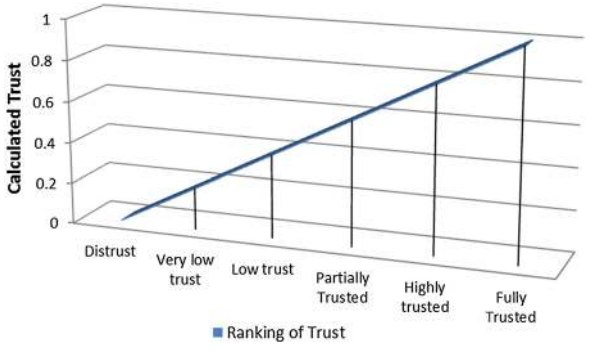

Fig. 1 Ranking of trust level

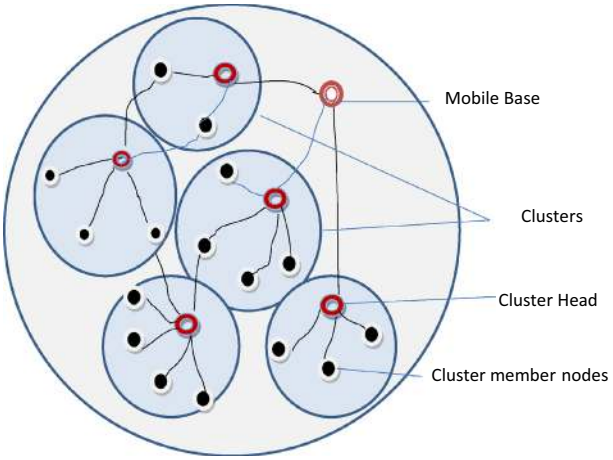

Fig. 2 Cluster

SensorSimulator is able to handle the traffic and the events generated in a better fashion so as to complete the simulation in a reasonable time faster than OPNet.

We observe that as number of nodes increase the signal strength attenuation also increase with more attacker cluster nodes. Based on the proposed methodology trusted cluster security can be viewed in Figs. 3 and 4, whereas the number of nodes in cluster increases the number of malicious nodes also increases but due to snooping based node detection and trust computation where if a nodes fails as per pre-defined threshold for each trust parameters than it is rejected so that trusted cluster security can be maintained (Fig. 4).

To study corresponding dynamics of energy saving, we found the average energy consumption with different escalating packets transmission range over a time with probability of node mobility. Energy consumption is lowest for different scenarios as Fig. 5 shows.

Comparison with traditional work Motivation of proposed work for human centric pervasive healthcare scenario asserts trust in human notion. We believe that acceptance

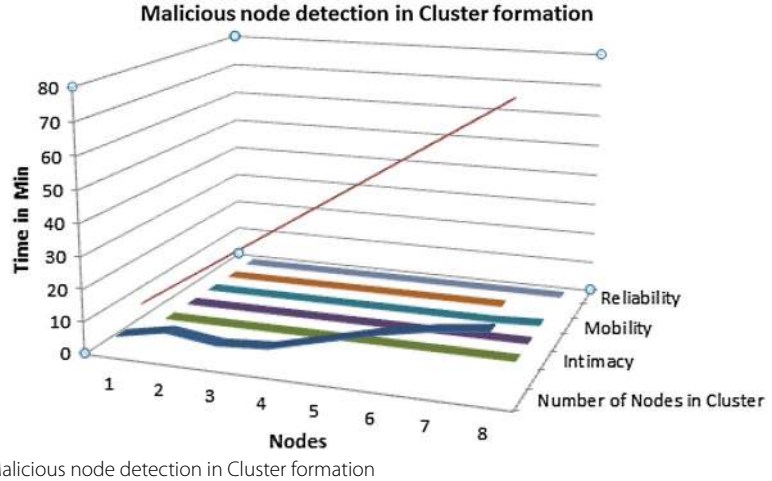

Fig. 3 Malicious node detection in Cluster formation

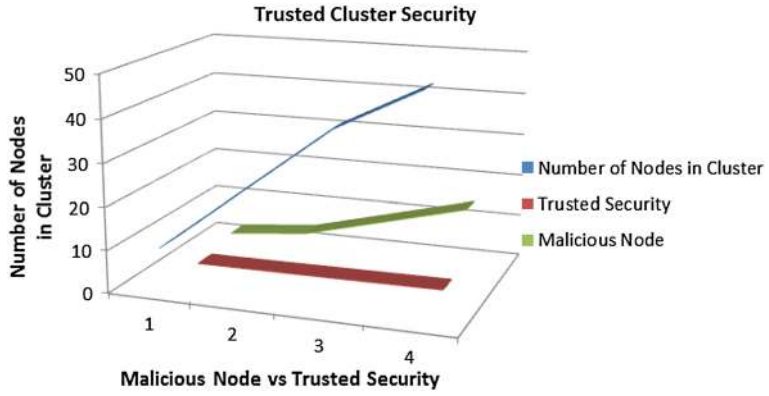

Fig. 4 Trusted cluster security

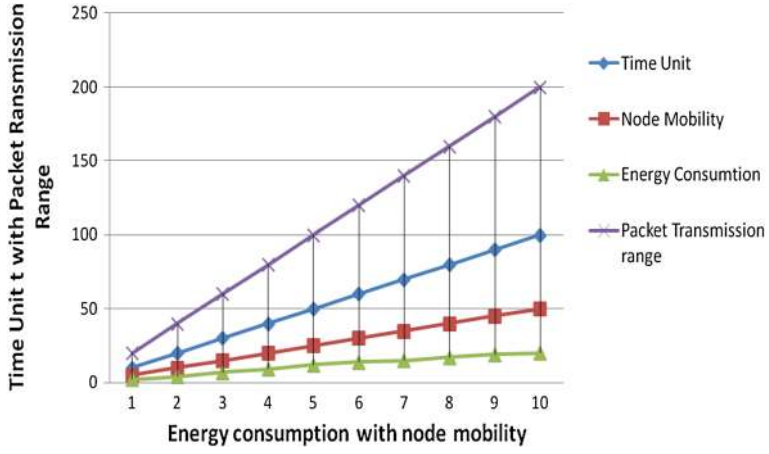

Fig. 5 Lowest energy consumption

of critical human-centric systems can be accepted by enhancing the security assurance based on QoS and Social trust parameters. There are various trust management systems are available with or without clustering for distributed, hybrid WSN and MANETs. We explored different traditional trust management systems and present their comparison as shown in Table 3.

In PTM [16], existing trust models have been explored and limitations to be applied to pervasive computing defined. It considers trust as the base of the inter-domain relationships in any community and presents the decentralized and automatic management of trust relationships for PerNets. Here trust changes dynamically, according to the entity's behavior and minimize the human intervention since most security management functions can be performed automatically with a trust based access control system, called TrustAC. It also measure the time and the battery consumption required to establish a trust relationship with and without recommendations, Finally, PTM has been proposed to provide a secure service discovery protocol to define policies and less storage of the historical behavior as it records a summary.

Table 3 Cluster based trust management system in open networks

Trust Mgmt. system	Trust value	Trust metric parameters	Type of trust (direct/indirect)	Network environment	Clustered/ non clustered
PTM-2004 [16]	0–1	Past experiences	Direct and indirect	Pervasive environment	Non clustered
GBTMS-2009 [12]	0–1	Past interactions	Direct and indirect	Hybrid	Clustered
HTM-2012 [2]	0–1	QoS and social	Direct and indirect	Hybrid	Clustered
LTD-2013 [24]	0–10	Successful interactions	Direct and indirect	Hybrid	Clustered

Standard clustering technique is used to reduce the resource consumption based on existing energy efficient approach LEACH (Low Energy Adaptive Clustering Hierarchy) one of the well-known cluster based protocol used to minimize the energy consumption in sensor networks. In LEACH randomly cluster head is selected from sensor and at the time of communication a sensor node and base station, energy is spread to all the sensor nodes in the network. The operation of LEACH deals with two important phases, set-up phase and steady phase. During the set-up phase, a random number between 0 and 1 will be selected by sensor nodes. The sensor node becomes cluster head, only if random number is less than the calculated threshold.

GBTMS [12] calculates the trust values on the basis of number of successful and unsuccessful interactions between nodes and indirect observations. It represents the recommendations of trusted peers. Each cluster head evaluates other cluster heads and sensor nodes under its cluster with major advantage of less memory consumption for group of nodes trust evaluation. Itt relies on broadcast based strategy and also the trust is calculated based on the past interaction experiences in message delivery. A node may build reputation and start behaving maliciously. But this paper assumes that a good node is always honest.

In HTM (hierarchical trust management) [2], to deal with selfish and malicious nodes trust management protocol was proposed. It Consider both QoS trust and social trust to judge if a node is trust worthy. A novel probability model called stochastic petri net is used to find the baseline truth character. It dynamically observe from past experiences and adapt to changing environmental conditions to maximize the application performance by addressing critical issues of hierarchical trust management namely trust composition, aggregation, and formation. The objective trust derived from global knowledge or ground truth derived that can be compared and validated against the subjective trust obtained as result of executing the trust management protocol.

A cluster based lightweight dependable trust, LTD l [24] is proposed to reduce the effects of malicious, selfish nodes a communication overheads for WSN. Trust has been evaluated for cluster head node and member nodes through feedback using self-adaptive Weighting method for trust aggregation. To obtain a global trust degree cluster heads is selected. There is no flooding problem because there is no broadcast communication. It is applicable in various wireless sensor network applications. In general most of the trust management approach uses weighted average to aggregate the trust value based on feedback without considering the dynamic malicious feedback that may lead to oversight trust decision making.

However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability with complex global trust degree evaluation algorithms used for cluster head selection. In [25–28] proposed work outlines significant contribution for maintaining the integrity and providing secure information exchange in pervasive networks. Need of combined intrusion detection and energy efficient trusted secure system proposed with clustering for the simultaneous resource efficiency and dependability. Open and dynamic networks are easy to be attacked by the way that traditional networks have never met. Here node may capture Eaves Dropping, sniffed, deny of service, worm hole and Sybil attack etc. The resource efficiency and dependability of a trust system are the most fundamental requirements for such highly dynamic and heterogeneous environment. In most of the existing trust mechanisms, trust management systems collect remote feedback and then the feedbacks from all the nodes are aggregated to obtain the global reputation which can be used to evaluate the global trust degree of the subjective node. Another reason is broadcast nature of the open environment; it contains a large number of malicious nodes. Feedback from these undependable nodes may result in the incorrect evaluation of feedback. So a trust system should be highly dependable in terms of providing service in an open WSN environment.

Contribution of proposed approach Main contribution of the proposed approach is to obtain a practicable degree of tradeoffs between the trust and security. QoS and Social trust metric parameters intimacy, integrity, mobility, selfishness and reliability identified and combined to evaluate the cumulative trust to provide ground level of security for human centric application with human notions. Unlike discussed trust management systems in order to growing years wise advanced technology [2, 12, 16, 24], we put forward our efforts to combine best of existing trust management models for soft security concerns while dynamically observing the impetus behavior of a node in open and dynamic pervasive environment. Exiting models are based on one or more trust or security parameters for WSN or MANETS, while our trust metric consists of five crucial trust parameters for direct and indirect communication in pervasive environment. To reduce the overheads and dependency clustering is used for group based communication.

Conclusion and future work

We proposed a trusted and secure energy-efficient clustering in mobile pervasive environment based on monitoring the dynamic impulsive behavior of nodes to become compromised. Since trust is an integral component in human centric application like pervasive healthcare thus acceptance of such applications can be by increasing the level of trust and security. Inspired from multi-objective optimization we formulate fitness functions to find out multi- dimension clustering with extended security consideration to improve energy efficient trusted clustering. Developing and Implementation of a Test bed using open source tools and technology regardless of device design are future steps to be taken.

Abbreviations

HEED: hybrid, energy-efficient, distributed; LEACH: low energy adaptive clustering hierarchy; PTM: a pervasive trust management; MTM: mobile trusted module; TPM: trusted platform module; TCG: trusted computing group; TCBMA: time constrained bee's mating approach; QoS: quality of services; WSN: wireless sensor networks; Wi-Fi: wireless fidelity.

Authors' contributions
In order to carry out our research work each author has an appropriate contribution in the proposed work. MSG has explore the literature in subjective area as per the guidelines provided by the BP (research guide) as a part of substantial intellectual contributions to the proposed study. To qualify and quantify the concept and approach, acquisition of data, or analysis and interpretation by simulation have been done and presented as a manuscript by MSG. We agree and accountable for all aspects of the work. Both authors read and approved the final manuscript.

Authors' information
Mrs. Madhu Sharma Gaur is MCA, M.Tech. and Perusing Ph.D. from Graphic Era University, Dehradun, Uttaranchal, India and working as Associate prof. at G.L. Bajaj Institute of Technology and Management, Greater Noida, UP India. She is serving IT industry as trainer academician and researcher from last 16 + years. Her areas of interest include Object Oriented Systems,.Net Technology and Trust and security in mobile pervasive environment.
Dr. Bhaskar Pant is Ph.D. from Maulana Azad National Institute of Technology, Bhopal, India and working as Associate Professor in the Department of Computer Science/Information Technology. His research interests in Data Mining, Machine Learning, soft Computing and Bioinformatics.

Author details
[1] GEU, Dehradun, India. [2] G. L. Bajaj Institute of Technology and Management, Greater Noida, India. [3] Department of IT, GEU, Dehradun, India.

Acknowledgements
We would like to express deep gratitude to Dr. R.C. Joshi Ex. Prof. E. and C.E. Department at IIT Roorkee and Chancellor at Graphic Era University Dehradun for his valuable support and guidance in exploring relevant literature and continuous improvements in the proposed research. We are also grateful Dr. Rajeev Agrawal, Director G.L. Bajaj Institute of Technology and Management, Greater Noida for providing significant insights of subjective, mathematical formulation and simulation and at last but not the least Dr. Amal Shankar Shukla for consistently helping and motivating.

Competing interests
The authors declare that they have no competing interests.

Received: 18 May 2015 Accepted: 4 October 2015
Published online: 31 October 2015

References
1. Weiser M (1991) The computer for the 21st century. Sci Am 265(3):94–104
2. Bao F, Chen IR, Chang MJ, Cho JH (2012) Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. In: IEEE transactions on network and service management, vol. 9, no. 2
3. Liu Lung, Liu Tang J, Yu FR, Lung C-H, Tang H (2009) Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. IEEE Trans Wireless Commun. 8:806–815
4. Cho J-H, Swami A, Chen I-R (2011) A survey of trust management for Mobile Ad hoc networks. IEEE Commun Surv Tutor 13(4):562–583
5. Cho JH, Swami A, Chen IR (2011) A survey on trust management for mobile ad hoc networks. IEEE Commun Surv Tutor 13(4):562–583
6. Velloso PB et al (2010) Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Trans Netw Ser Manag 7(3):172–185
7. Ali H, Shahzad W, Khan FA (2012) Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Applied Soft Computing 12:1913–1928
8. Hsieh MY, Huang YM, Chao HC (2007) Adaptive security design with malicious node detection in cluster-based sensor networks. Comput Commun 30:2385–2400
9. Trusted Computing Group, Mobile Phone Work Group (2009) Selected use case analyses—v 1.0
10. TCG (2010) TCG MPWG mobile trusted module specification, version 1.0, Revision 7.02 29
11. Bu S, Yu F, Liu X, Mason P, Tang H (2011) Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks In: IEEE Trans, vehicular technology, vol. 60, no. 3
12. Ghorbel M, Ahamed A, Mokhtari M (2009) Secured and trusted service provision in pervasive environment. In: IEEE international conference on wireless and mobile computing, networking and communications
13. Ali IA, El-Haleem AMA (2011) TRIUMF: trust-based routing protocol with controlled degree of selfishness for securing MANET against packet dropping attack. IJCSI Int J Comput Sci Issues, vol 8, Issue 4, No 1, ISSN (Online).pp 1694–0814
14. Yuan B, Herbert J (2011) Web-based real-time remote monitoring for pervasive healthcare, pervasive computing and communications Workshops. In: IEEE International Conference, pp 625–629
15. Lopez J, Roman R, Agudo I, Fernandez CG (2010) Trust management systems for wireless sensor networks: best practices. Comput Commun 33:1086–1093
16. Almenarez F, Marin A, Campo C, Garcia RC (2004) PTM: a pervasive trust management model for dynamic open environments. In: Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust; Boston, MA, USA
17. Almenarez F, Marin A, Diaz D, Sanchez J (2006) Developing a model for trust management in pervasive devices. In: Proceedings of 4th IEEE Annual International Conference on Pervasive Computing and Communications, Pisa, Italy, pp. 267–271

18. Almenarez F, Marin A, Campo C, Garcia RC (2005) Trust AC: trust-based access control for pervasive devices. In: Proceedings of the 2nd International Conference on Security in Pervasive Computing; Boppard, Germany, pp 225–238
19. IEE Std. 802.11, 1999 Edition, r2003 ed., 1999
20. Bharghavan V, Demers A, Shenker S, Zhang L (1994) Macaw: a media access protocol for wireless lan's, in Proceedings of the conference on Communications architectures, protocols and applications ACM Press, pp 212–225
21. Velloso PB et al (2010) Trust management in mobile ad hoc networks using a scalable maturity-based model. In: IEEE Trans. Netw. Service Management, vol. 7, no. 3, pp 172–185
22. Ali H, Shahzad W, Khan FA (2012) Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Applied Soft Computing 1913–1928
23. Marmol FG, Perez GM (2010) Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Comput Stand Interfaces 32:185–196
24. Li X, Zhou F, Du J (2013) LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. In: IEEE Transactions on Information Forensics and Security, vol. 8, no. 6
25. Li JL, Gu LZ, Yang YX (2009) A new trust management model for P2P networks. J Beijing Univ Posts Telecommun 32:71–74
26. Achankunju M, Pushpalakshmi R (2013) Quality of service based secure clustering for mobile adhoc networks using particle swarm optimization. In: ITEE, vol 2, Issue 3, ISSN: 2306-708X
27. Bu S, Yu F, Liu X, Mason P, Tang H (2011) Distributed Combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. In: IEEE Trans, vehicular technology, vol. 60, no. 3
28. Titi X, Lafuente CB, Seigneur JM (2011) Trust management for selecting trustworthy access points. IJCSI Int J Comput Sci Issues, vol 8, issue 2, ISSN (Online): 1694–0814