International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32663-32679

http://www.ripublication.com

A Novel And Efficient Hybrid Authenticated Trust Mechanism For Clustered Wireless Sensor Network

R.Sivakumar[1] and Dr. S.Duraisamy[2]

[1] Assistant Professor, [2]Professor & Head
[1]Department of MCA [1]SNS College of Technology
[1]Coimbatore-641035 India
[1]sivakumar.rphd@gmail.com

Abstract

In recent times, preservation security and confidentiality in Wireless Sensor Networks (WSN) are extremely vital and challenging. In comparison with wired networks, WSNs are largely susceptible to the attacks and intrusions. In case of WSN, an unknown person can possibly eavesdrop to the data or connection to the network. As a result, detection and stopping these intrusions has turned out to be one of the most demanding challenges. The clustered WSNs are not sufficiently expert in meeting the resource efficiency and trust system as a consequence of the high overhead and low dependability. Several trust systems are employed in WSN which makes use of the clustering algorithm. The latest trust system makes use of a self-adaptive feedback scheme for the purpose of trust evaluation. Although this makes an attempt to enhance the energy effectiveness and substantiates the trustworthiness of nodes that take part in the communication, there still exist certain serious drawbacks. The trust values can be estimated by an unauthorized person and moreover there is no authentication during the transmission of messages. Hence, a novel trust mechanism called Hybrid Authenticated Trust System (HATS) is formulated which includes two level of trust mechanism in order to enhance the security and confidentiality between the nodes, moreover helps in energy saving and helps in reducing the data transmission redundancy. The trust constraints like packet delivery ratio and honesty of the nodes are largely employed in this trust system which is recognizable and computable at any stage in network events. In this system, trust value of its neighbors is computed which is derived from two information sources i.e., direct and indirect observations. Every cluster comprises a watchdog mechanism that permits it to observe the network events of cluster members. An additional objective is to considerably lessen the cost related with trust evaluation as compared against distributed schemes. The proposed system is simulated in NS2 and the performance of the HATS is compared against other latest standard approaches.

Keywords: Direct Observation, Indirect Observation, Light Weight and Dependable Trust System, Wireless Sensor Networks

1. Introduction

Wireless Sensor Networks (WSNs) comprises of numerous small tools that are used for the purpose of communication, sensing and processing potentials to observe the real-world atmosphere. The WSN are greatly helpful in the field o military applications. In case of these applications, a huge amount of sensor nodes are organized for the purpose of monitoring a huge field in a hostile surrounding. Currently, in the majority of WSN applications, the complete network must possess the capability to control vigorous situations where human right of entry and observation cannot be scheduled or effectively controlled or it's even not practicable at all [1]. Due to this critical prospect, in numerous WSN applications the sensor nodes are habitually organized arbitrarily in the region of interest by fairly uncontrolled means (i.e., put down through a helicopter) and they generate a network in an ad hoc behavior [2, 3]. In addition, the complete region that has to be covered up, the small extent of the battery energy of the sensor nodes and the chance of comprising broken nodes at some stage in the deployment phase, huge populations of sensors are anticipated; it's a likely chance that hundreds or might be thousands of sensor nodes will be engaged. Besides, sensors in these atmospheres are energy limited and their batteries cannot be recharged. Consequently, it's evident that dedicated energy-aware routing and data assembly protocols providing elevated scalability should be deployed with the intention that network lifetime is maintained adequately high in these situations.

In nature, gathering sensor nodes into clusters has been extensively implemented by the research group of people to meet the above mentioned scalability objective and accordingly realize high energy efficiency and extend network lifetime in large-scale WSN environments. The related hierarchical routing and data collection protocols involve cluster-based association of the sensor nodes with the intention that data fusion and aggregation are feasible, as a result leading to considerable energy savings. In case of the hierarchical network configuration, every cluster possess a leader, which is also known as the Cluster Head (CH) and typically carries out the unique operations like fusion and aggregation, and a number of normal Sensor Nodes (SN) as members.

For WSNs, it is observed that trust management is a supportive business more willingly than an individual task owing to the exploitation of clustering approaches like LEACH [4], PEGASIS [5], TEEN [6], and HEED [7] in real-world circumstances. Furthermore, SNs can also be organized in the manner of groups [8], which are ready to work together with each other so as to process, aggregate and transmit gathered data [9]. This emphasizes the information that these clustering approaches and group deployments allow SNs to accomplish their duties in a supportive manner more willingly than individually. Consequently, establishing and supervising trust in a cooperative approach in clustering atmosphere offers several benefits, like, inside the cluster, it assists in the choosing of trusted cluster lead by the

member nodes. In the same way, the CH will be potential enough sense defective or malicious node(s). In the scenario of multihop clustering, it assists in selecting trusted en route nodes through which a node can transmit data to the CH. At some stage in intercluster communication, trust management assists to choose trusted en route gateway nodes or additional trusted CHs by means of which the sender node will transmit data to the Base Station (BS).

Several trust management approaches have been formulated for the purpose of peer-to-peer networks and ad hoc networks. On the other hand, a small number of comprehensive trust management approaches (e.g., Agent-based Trust and Reputation Management (ATRM), Reputation-based Framework for Sensor Networks (RFSN), and Parameterized and Localized trUst (PLUS) have been formulated for sensor networks. Even though, there are few other researches available in the next section discusses trust however not in much detail. According to the literature, only ATRM approach is exclusively constructed for the clustered WSNs. On the other hand, even ATRM and other approaches experience different drawbacks like they do not satisfy the resource constraint prerequisites of the WSNs and, more explicitly in the scenario of large-scale WSNs. In addition, these approaches experience from higher cost connected with trust evaluation in particular of distant nodes. Moreover, existing approaches have certain other drawbacks like reliant on particular routing approach, like PLUS functions on the crown of the PLUS_R routing approach; reliant on particular platform, for instance, the ATRM approach needs an agent-based platform; and impractical suppositions, similar to the ATRM presumes that agents are flexible in opposition to any security attacks, and so forth. As a result, these schemes are not adequately suited for sensible WSN applications.

Although this kind of approaches provides considerable energy efficiency and confirms the trustworthiness of nodes that take part in the communication, there are many drawbacks. The trust values can be evaluated by an third person or an intruder and in addition there is no authentication for the information being sent through nodes. In order to overcome these complications, a new framework is formulated in this paper intended for secure Clustered Wireless Sensor Networks.

2. Related Works

Ganeriwal and Srivastava [10] formulated RFSN, in which each SN preserves the status for the corresponding neighboring nodes only. Trust values are computed in accordance with the status and they employ Bayesian formulation for indicating the status of a node. RFSN presumes that the node has adequate communications with the neighbors with the intention that the status (beta distribution) can arrive at a stationary state. On the other hand, when the degree of node mobility is maximum, status information will not become constant. In case of RFSN, no node is permitted to distribute bad reputation information. When it is presumed that “bad” status is unconditionally included by not broadcasting good status, then in this scenario, this approach will not be capable of handling with uncertain circumstances [14].

Boukerche et al. [11] have formulated an ATRM approach for WSNs. ATRM depends on a clustered WSN and analyzes trust in a completely distributed way.

ATRM functions on particular agent-based platform. In addition, it presumes that it includes a single trusted authority, which is accountable for constructing and initiating mobile agents, which enables it weak against a single point of breakdown. ATRM also presumes that mobile agents are flexible against malicious nodes that attempt to steal or transform data carried by the agent. In several applications, this assumption might not be practical.

Yao et al. [12] have formulated PLUS for WSN security. Here implemented a localized distributed scheme and trust is computed in accordance with either direct or indirect observations. This approach works on top of its defined routing approach called PLUS_R. In this approach, the authors presume that the entire vital control packets produced by the BS must include a Hashed Sequence Number (HSN). Insertion of HSN together with control packets not only enlarges the size of packets, at the same time resulting in elevated utilization of transmission and reception power and also raises the computational cost. In addition, at any time a judge node receives a packet from another node, it will constantly test out the integrity of the packet. When the integrity assessment is not pass, subsequently the trust value of node will be diminished irrespective of whether node was actually engaged in maliciously making certain alteration in a packet or not.

Liu et al. [13] have formulated an extremely uncomplicated trust management approach for Resilient Geographic Routing (T-RGR). This approach works in a completely distributed manner, where all nodes monitor the activities of onehop neighbors. In case of the T-RGR scheme, authors have employed several predetermined threshold values that put together their approach nonadaptive. In addition, each node only depends on its direct monitoring in order to calculate trust value, which causes it vulnerable in case of collaborative attacks.

Zhan, et al. [15] formulated a Trust-Aware Routing Framework (TARF) for WSNs, it is a robust framework for the use in dynamic WSNs. Even there is no tight time synchronization or recognized geographic information, TARF offers trustworthy and energy-efficient routing. Furthermore, TARF is extremely successful in opposition to the destructive attacks programmed out of identity deception; the flexibility of TARF is established through wide-ranging evaluation with both simulation and empirical assessments on large scale WSNs under different scenarios.

Baoet al. [9] formulated a Hierarchical dynamic Trust Management Protocol (HTMP), for the purpose of effectively handling self-interested or malicious nodes. Multidimensional trust features obtained from communication and social networks are taken to assess the overall trust of a sensor node. A probability model making use of a stochastic Petri nets scheme for the purpose of analyzing the protocol working, and also assess subjective trust in opposition to objective trust obtained in accordance with the ground truth node status. Implementation of such a complex trust evaluation approach at every CM of the cluster is extremely impractical.

Crosby et al. [16] formulated a scheme called TCHEM, which is a distributed trust-based scheme and a method for the selection of trustworthy CH. This scheme considerably reduces the possibility of compromised or malicious nodes from being chosen as CHs. TCHEM does not offer trust in depth, in view of the fact that several key issues of trust management are not taken into account.

3. Proposed Methodology

The resource effectiveness and reliability of a trust system should unquestionably be the most primary constraints for any WSN (together with clustered WSNs). On the other hand, existing trust systems formulated for clustered WSNs are not capable of meeting these constraints, as a consequence of their elevated overhead and low reliability [17]. In this paper, a novel trust mechanism is formulated which includes two level of trust scheme for enhancing the communication among the nodes, by energy saving (at the time of data transmission) and in the mean time reducing data transmission redundancy. The trust constraints like packet delivery ratio (pdr) and honesty of the nodes are predominantly employed in the proposed trust system which is recognizable and measurable at some stage in network events. In this scheme, trust value of its neighbors is computed in accordance with the two information sources i.e., direct observations and indirect observations. Every cluster includes a watchdog mechanism that permits it to examine the network incidents of cluster members. The major intention of this scheme is to considerably diminish the cost related with trust evaluation as compared against distributed approaches.

3.1. Message Authentication

In this scheme, the complete packet transfer among the source nodes to destination node or intermediary node is encrypted with the assistance of RSA algorithm.

Key generation

RSA makes use of a public key and a private key. The public key is revealed to all and is utilized for the purpose of encrypting messages. Messages encrypted with the assistance of the public key can only be decrypted with the help of private key. The keys for the RSA algorithm are constructed using the following manner:

1. Select two dissimilar prime numbers p and q. In order to perform securely, the integers p and q should be selected arbitrarily, and must be of equal bit-length.
2. Calculate $n = pq.n$ which is employed as the modulus for both the public and private keys.
3. Work out $\varphi(n) = (p-1)(q-1)$, in which φ represents Euler's totient function.
4. Pick an integer e in order that $1 < e < \varphi(n)$ and $gcd(e, \varphi(n))$ are co-prime. e is made public as the public key exponent.
5. Find out $d = e^{-1} mod \varphi(n)$; i.e., d represents the multiplicative inverse of $e \ mod \ \varphi(n)$. d is reserved as the private key exponent.

Encryption algorithm

Receiver sends out public key (n, e) to sender and preserves the private key as secret. Subsequently, sender desires to transmit message M to receiver. During the process, it initially turns M into an integer m, in order that $0 < m < n$ with the help of an agreed-upon reversible protocol called as a padding scheme. It subsequently works out the cipher text c similar to,

$$c = m^e (mod\ n)$$

Decryption:
Receiver can recover m from c with the help of the private key exponent d via computing

$$m = c^d (mod\ n)$$

By knowing m, receiver can recover the original message M by reversing the padding scheme.

3.2. Trust Evaluation

Intra-Cluster Trust Evaluation
A source node computes the trust value of its neighbors or cluster members in accordance with two information sources, specifically, direct and indirect observation. Direct trust degree indicates the trust evaluation of its nearby nodes through source node and indirect trust degree indicates the trust assessment by CH. Parameters like honesty, PDR are computed with the help of watchdog mechanism. The separate table is kept by CH and source node for the purpose of computing the trust value of each node within the cluster.

Direct observation
The entire nodes in cluster contact by means of a shared bidirectional wireless channel and function in the promiscuous approach. When source node transmits the incessant message to the nearby nodes within particular time Δt, subsequently the packets delivered and amount of packets dropped are calculated in accordance with the ACK received by the source node inside Δt.

$$d_i = (1 - \mu)\frac{N_s}{N_t}$$

Where μ denotes smoothing constant, N_s indicates a number of packet received effectively and N_T denotes a overall number of packets transmitted. In this work, direct observation is taken as the link quality measurement among the source node and intermediary node. All links among the nodes is computed with the intention of finding the trust value of the nearby nodes. The link cost is characterized as the converse of the delivery ratio (d) of continuous packets transmitted successfully to the nearby node. In particular, the cost (C) of link $A \rightarrow B$ is computed as,

$$C = \frac{1}{d_i}\ and\ d_i = (1 - \mu) \times d_{i-1} + \mu \times \frac{N_s}{N_t}$$

Where N_s indicates the successful sending of packets to nearby node, N_t indicates a total number of packets transmitted to the nearby node. The confirmation is obtained by source node from the target node, based on that the number of packets delivered can be computed. In accordance with this the reputation value of every node is computed in the trust model and it is taken as direct observation value. The

computed reputation or trust value is accumulated in table format for further future communications.

Indirect observation

In the proposed scheme, a network that comprises of clusters is taken into consideration. The node with maximum energy is regarded as a CH and is dynamically allocated in accordance with the energy considerations of the entire nodes in the cluster. The cluster members are supervised with the help of watchdog mechanism. In this scheme, CH perform as watchdog and overhears the cluster member messages.

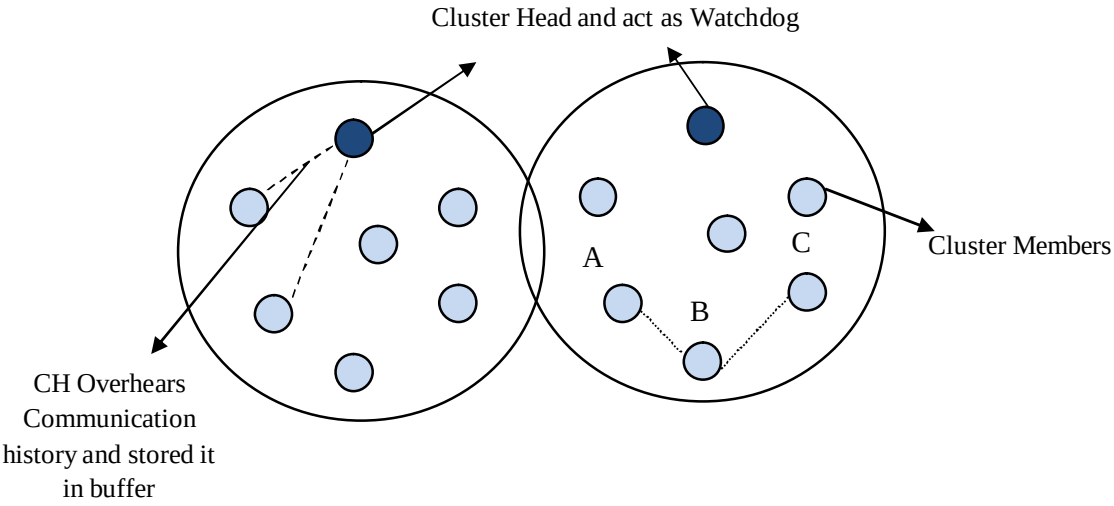

Figure 1: CH operates as a Watchdog in proposed mechanism

Honesty value calculation

The CH typically gathers and aggregates data regarding sensor nodes in its own cluster and preserves the information in a table arrangement. In the proposed scheme, the CH preserves information regarding the trust constraint like honesty value of the entire nodes. In the network model, consider the nodes A, B and C in the second cluster are used for communication. If node A transmits the information to node B, automatic timer is initiated for the purpose of computing the packet delay. The CH node observes the transmission of cluster members inside its cluster limit, it means it will overhear the transmission of the entire cluster members. The packet must be transmitted inside the real time delay, or else the malicious node count for node B will be increased and CH will request the source to retransmit the packet to the node B. At this point, the malicious node count is taken as an honesty value and it is accumulated as table in CH. When the honesty count of a node attains the threshold value, the node will be confirmed as malicious by CH and the message will be transmitted in the cluster. The honesty value of the entire node is computed in the time gap Δt. The honesty value in CH is employed for future communication since time based precedent interaction value which provides the suggestions for secure communication.

Packet delivery calculation

The CH transmits a succession of the packet with size S and length L to passes into every node exists inside the network. When the neighboring node obtains the series packets, the time spacing among the reception of initial and very last packet is computed. The packet delivery time is computed by means of the formula

$$packet\ delivery\ = transmission\ time + propogation\ delay$$

In the mean time, the transmission time is computed as,

$$transmission\ time = packet\ size/bitrate$$

and

$$propogation\ delay = distance/propogation\ speed$$

The computed value is employed for recognizing the malicious actions of the node. When the node has maximum packet delivery at that time it is taken as trusted node.

$$T_{CH}^{x} = \begin{cases} \gamma H_{CH}^{x}(t) < th_h \\ \gamma PD_{CH}^{x}(t) > th_{pdr} \end{cases}$$

Where x indicates the amount of nodes in the cluster, γ represents a decay of trust $0 \leq \gamma \leq 1$, H_{CH}^{x} represents honest value of x computed by CH, t represents time period, PD_{CH}^{x} indicates pdr of the node x.

Inter-Cluster Trust Evaluation

During the process of inter cluster trust evaluation, the trust value of its neighbors CH is computed in accordance with two information sources, direct observations and indirect observation. The CH itself assesses the other CH trust value directly is regarded as direct observation. The BS supervises the entire nodes in the network by means of watchdog mechanism and computes the trust value for the entire nodes is regarded as indirect observation.

Direct observation

As described in the process of intra cluster, the CH transmits the continuous message to the nearby CH nodes inside time Δt, subsequently the packets delivered and amount of packets dropped are computed in accordance with the ACK received by the source node inside Δt.

$$d_i = (1 - \mu)\frac{N_s}{N_t}$$

At some stage in CH-to-CH communication, the CH preserves a table of past communications with some other CHs in the similar manner as CMs maintain records

of other CMs. In addition, the past communications are used in the trust computation by using the formula,

$$d_i = (1-\mu) \times d_{i-1} + \mu \times \frac{N_s}{N_t}$$

The acknowledgement is obtained by CH node from the destination CH node, based on that the amount of packets delivered can be found. In accordance with this the reputation value of every node can be computed in this trust model and it is taken as direct observation value. The computed reputation or trust value is accumulated in table format for further future interactions.

Indirect observation

In this model, BS takes action as a watchdog and overhears the CH communications.

The BS typically gathers and aggregates information regarding the entire nodes in network and preserves the information in a table arrangement. In this model, the BS preserves information of the entire nodes in the network. Here, the BS overhears the data transmission of the entire clusters. The BS computes the reputation value of the entire nodes by means of the two variables C certainty and uncertainty UC.

$$C = \min(Pd_i, Pd_j); C = \max(Pd_i, Pd_j);$$

$$UC = \min(H_i, H_j); UC = \max(H_i, H_j)$$

Where i and j represents the nodes in the network;

Then it is simple to determine the trust and untrust value, using the following equations.

$$C = \frac{avg(Pd_i, Pd_j)}{1 - \left(avg(Pd_i, H_j) + avg(Pd_j, H_i)\right)}$$

$$UC = \frac{avg(H_i, H_j)}{1 - \left(avg(Pd_i, H_j) + avg(Pd_j, H_i)\right)}$$

With the help of C and UC, it is easy to determine the evaluation level of sensor network in BS.

$$Evalauiton\ time = \frac{C}{C + UC}$$

The computed value is utilized for the purpose of recognizing the malicious activities of the node. Both certainty and uncertainty value are evaluated against the threshold value. When the certainty value is under the threshold value and the

uncertainty value is beyond the threshold value, subsequently it is taken as malicious node. The information regarding the malicious node is spread to other nodes by BS and the node is secluded from the network.

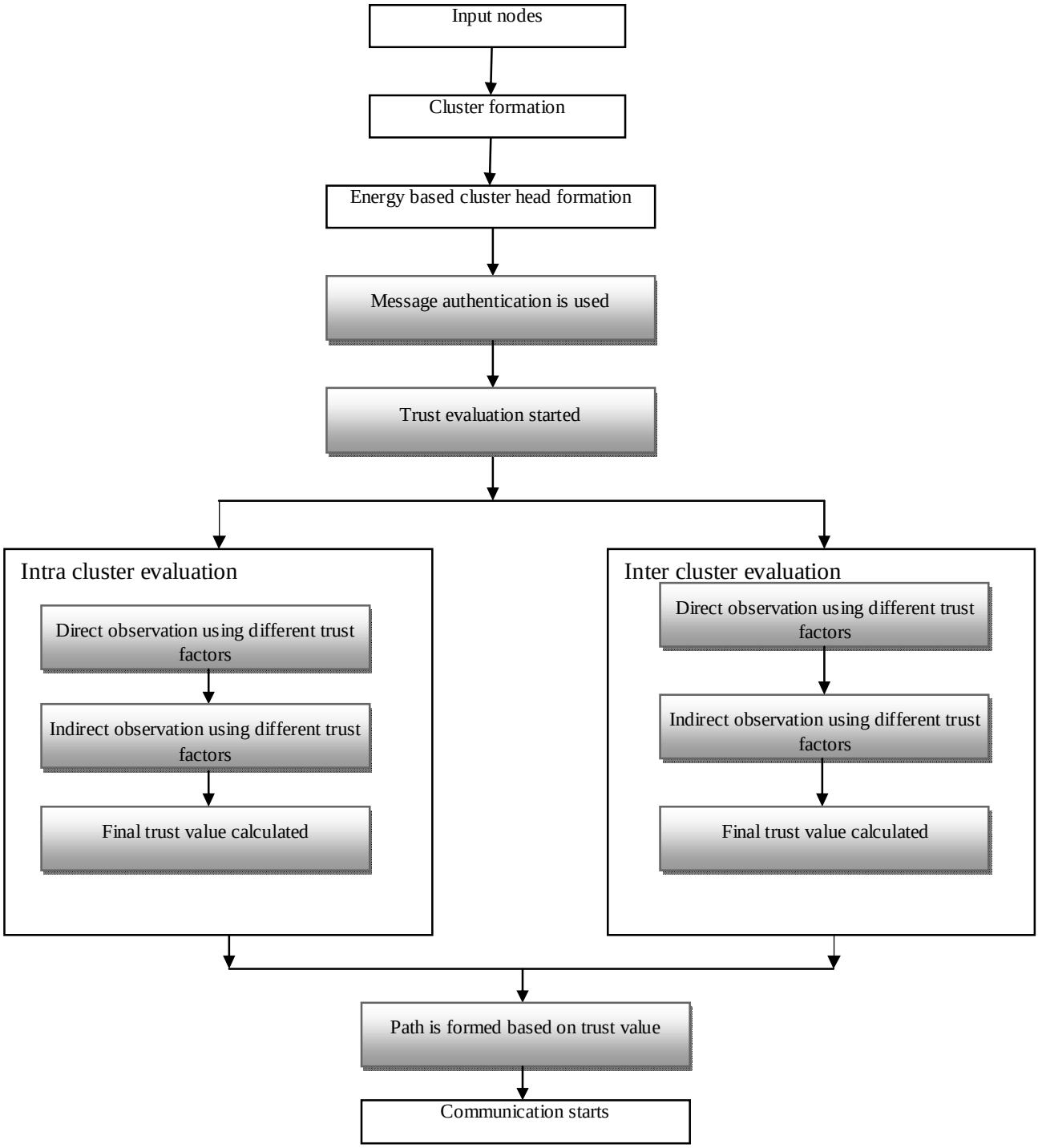

Figure 2: Overall Proposed Trust based Mechanism

3.3. Data Transmission

As soon as a source node gets ready to send out packets to a destination node by means of multihop communication, it must assess the trust value of the route. In general, the design of trust computation of paths is supposed to be complying with the following constraints. Initially, the trust information cannot be boosted via propagation. It means; the trust value of a path must not be more than the trust value of any intermediary node in the path. Then, the destination node is considered to be a trusted entity in trust management systems and its trust value for any other node in the path must be fixed to 1.

When the most trusted path is chosen which is determined by the maximum product of the entire trust values along the path, the trust of a path p can be calculated by using the following formula,

$$t(pa) = \prod (t(i,j) | i,j \in p, i \to j)$$

where node i and node j represent the neighbors. Node j indicates the next hop of node i.

The most trusted path is chosen which is determined by the highest minimum trust values of intermediary nodes in the path. The trust of a path p can be provided as follows:

$$t(pa) = \min(t(i,j) | i,j \in p, i \to j)$$

The function $min(*)$ provides the minimum value from the input set.

The in depth procedure of the trust-ware routing protocol works is given below.

Step 1. If the source node S gets ready to transmit packets to the destination node D, subsequently the node S initializes the trust evaluation process and transmits a request packet to its nearby nodes. The trust request is a 5-ary tuple and is given as TR

$$TR = \langle S_{id}, D_{id}, ts, s, hl \rangle$$

Where S_{id} indicates the source node's ID, D_{id} represents the destination node ID, ts denotes a time stamp, s represents sequence number of request packet forward to other nodes and hl is hop limit of trust request packet.

Step 2. As soon as obtaining the request packet, the destination nodes throws the ACK to the source node, subsequently the source node begins to trust evaluation process on destination node. At that moment, these nodes will drop the transmit trust request packets when the hop limit value is equal to zero.

Step 3. Subsequent to estimating the direct and indirect observation, the final trust value is computed. After that, source node can decide whether the destination node must be trusted in keeping with the required path trust constraint.

Step 4. When an intermediate node that obtains the route request that has the best possible route to the destination node, it will throw an ACK to the source node. At that moment, the source node can discover the optimal route to the destination node. Move to Step 6. If not, the intermediary trusted node will reiterate Steps 1–3 to discover the next trusted one.
Step 5. When the route request strikes the destination, the destination node will transmit a route response to the source node by means of the chosen reverse route.
Step 6. At last, node can transmit data packets to node through the optimal route.

4. Experimental Results

In this section, the NS-2 simulator is employed to assess the performance of proposed trust system Hybrid Authenticated Trust System (HATS). The simulations model a network comprising of 100 sensor nodes placed arbitrarily inside a $200m \times 200m$ area. Two categories of sensor nodes in the simulations: well-behaved nodes and malicious nodes. The malicious nodes can initiate tampering, greyhole, bad mouth and on-off attacks. Here, initially considered the impact on the network produced by each attack; subsequently the scenario that all the four malicious activities are initiated concurrently is also be analyzed. The BS has unrestricted energy. The number of selected CH is predetermined to 10% for one interval. The HATS performance is evaluated by comparing against the existing system like Light weight and Dependable Trust System (LDTS) and Group-based Trust Management Scheme (GTMS).

4.1. Packet delay ratio

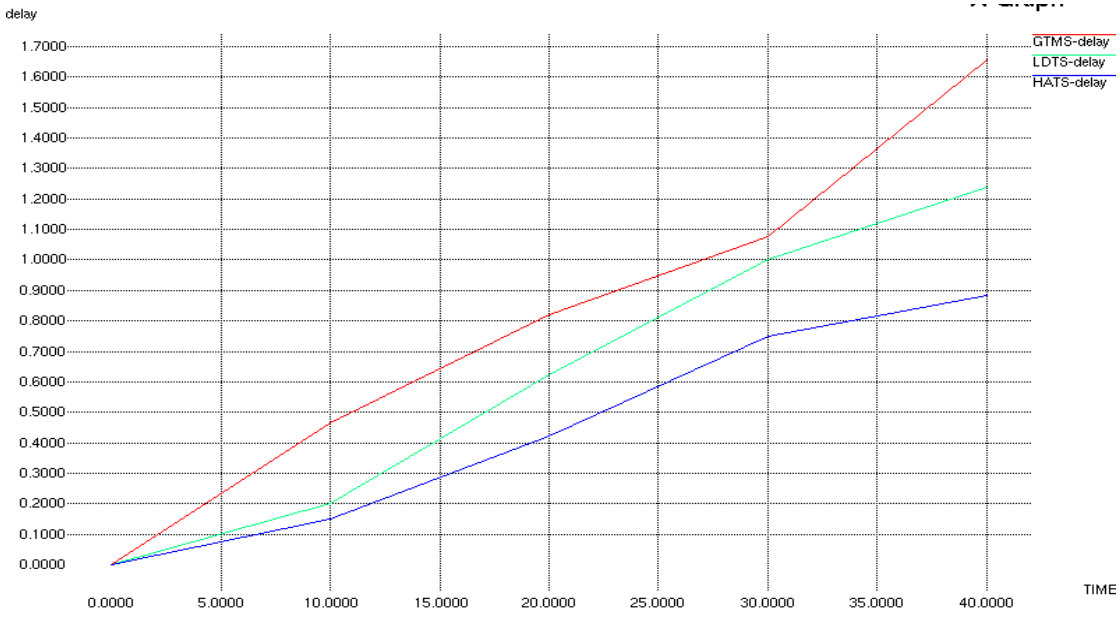

Figure 3: Comparison of Packet Delay for Different Trust Mechanism

The figure 3 shows the performance of proposed HATS compared LDTS and GTMS algorithm with respect to the time and packet delay ratio. As Fig in 3, the HATS scheme has lower packet delay than the existing LDTS and GTMS. Loss of packets or malfunction for proposed HATS is low, which shows better packet delay results.

4.2. Throughput

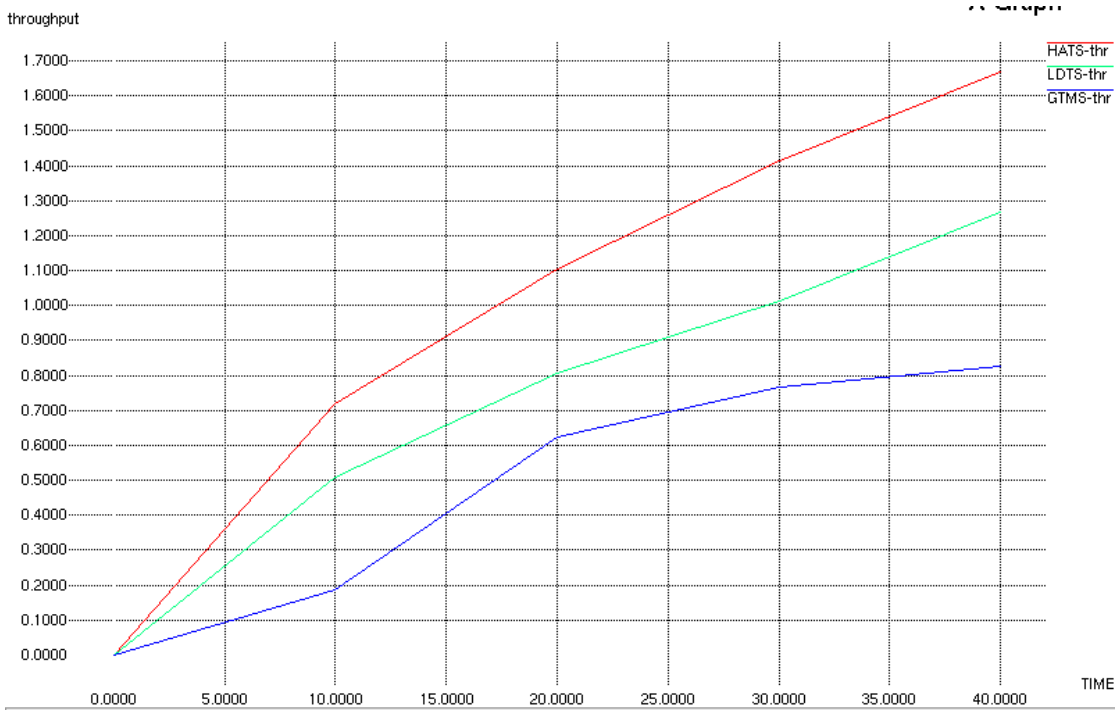

Figure 4 : Comparison of Throughput

The figure 4 shows the performance of proposed HATS compared LDTS and GTMS algorithm with respect to the time and throughput. As Fig in 4 , the HATS scheme has higher throughput than the existing LDTS and GTMS. Number of packets which is successfully obtained at the destination without any loss of packets or malfunction for proposed HATS is high, which shows better throughput results.

4.3. Packet delivery ratio

It is the ratio of the number of delivered data packet to the destination. This demonstrates the level of delivered data to the destination.

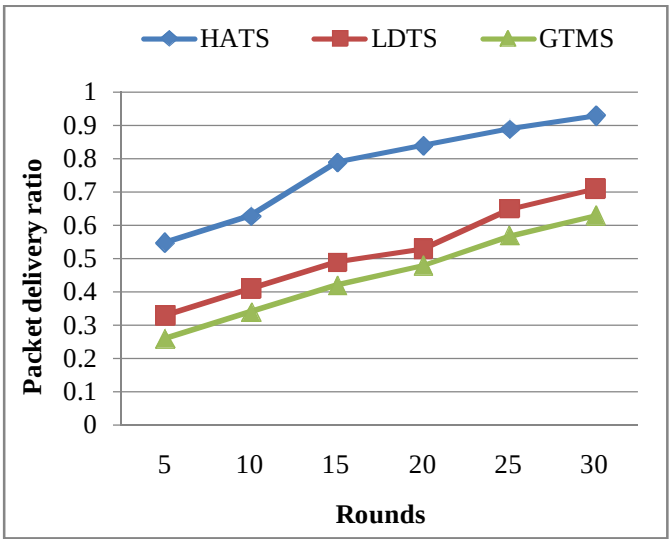

Figure 5: Packet Delivery Ratio vs Number of Nodes

The figure 5 shows the performance of proposed HATS compared LDTS and GTMS algorithm with respect to the number of rounds and packet delivery ratio. As Fig in 5, the HATS scheme has higher packet delivery ratio than the existing LDTS and GTMS. Number of packets which is successfully obtained at the destination without any loss of packets or malfunction for proposed HATS is high, which shows better pdr results. In the proposed HATS methods the pdr achieves maximum values, since the proposed routing is carried out on the basis hybrid trust system, which solves self-centered behavior problem promptly when compare to other schemes.

4.4. Average Time Spent On Routing Establishment

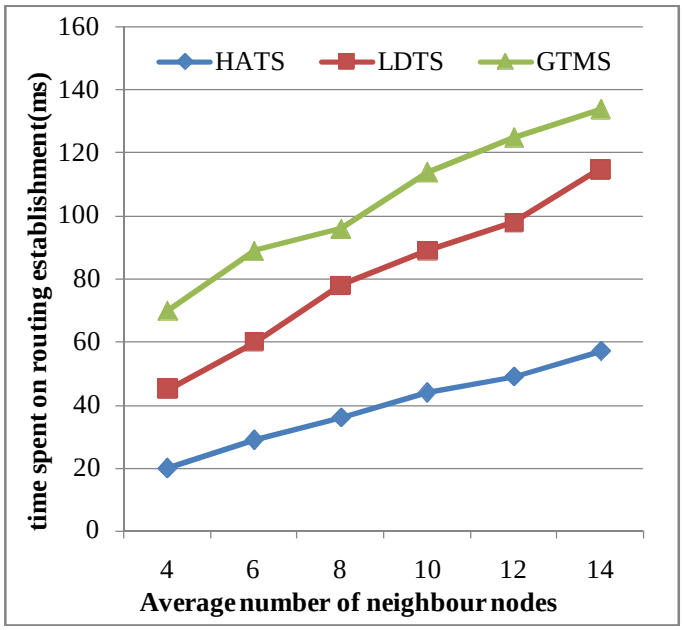

Figure 6 : Comparison of Time Spent on Routing Establishment

The figure 6 shows the comparison of time spent on routing establishment for proposed HATS, LDTS and GTMS algorithm with regard to the number of nodes. From the figure, it is found that the HATS method has low time when compared with the existing system LDTS and GTMS.

4.5. Detecting the Malicious Nodes

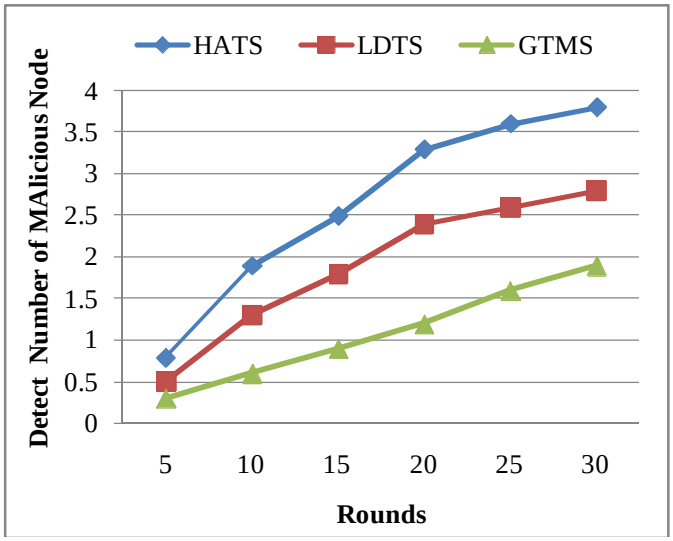

Figure7: Number of Malicious Nodes

The performance of proposed HATS compared LDTS and GTMS algorithm with regard to the number of rounds and discovery of malicious nodes. As Fig.7 shows, the proposed method detects the entire compromised nodes after about 8 rounds. The network consistency is one of the significant constraints of sensor networks. These constraints can be described in terms of the network capacity in sensing the events at some stage in the network lifetime. The more a network supervises to discover events (or the less it loses the events), then its reliability is maximum.

5. Conclusion

This model can significantly enhance the system effectiveness, at the same time as dropping the consequence of malicious nodes. By means of adopting an enhanced trust evaluating approach for cooperation's among nodes, HATS can successfully sense and stop selfish, malicious and defective nodes. During its process, each and every message at some stage in data transmission are authenticated by means of RSA algorithm for secure communication, this scheme can considerably improve the system efficiency at the same time as reducing the consequence of malicious nodes. The HATS scheme has employed two stage of trust mechanism. The direct trust value and indirect trust value is computed before beginning the communication. The proposed secure protocol can be employed in the majority of applications, not only one-to-one secure transmission, however also for broadcasting and multicasting. Simulation results reveal that this scheme insists less memory and communication overhead as compared against other typical trust systems and is extremely appropriate for clustered WSNs.

Reference

[1] Abbasi, A.A., and Younis M., 2007, "A survey on clustering algorithms for wireless sensor networks", Computer Communications, 30: pp.2826-2841.

[2] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., 2000, "Protocols for self-organization of a wireless sensor network", IEEE Personal Communications, 7(5), pp.16–27.

[3] Min, R., Bhardwaj, M., Cho, S. H., Shih, E., Sinha, A., Wang, A., and Chandrakasan, A., 2001, "Low power wireless sensor networks", in Proceedings of International Conference on VLSI Design, Bangalore, India, pp. 205-210.

[4] Heinzelman, W. B., Chandrakasan, A. P., and Balakrishnan, H., 2002, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., 1(4), pp. 660-670.

[5] Lindsey, S., and Raghavendra, C. S., 2002, "PEGASIS— Power-Efficient Gathering in Sensor Information Systems," Proc. IEEE Aerospace Conf., 3, pp. 1125-1130.

[6] Manjeshwar, A., and Agrawal, D. P., 2001, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proc. 15th Int'l Parallel and Distributed Processing Symp., pp. 2009-2015.

[7] Younis, O., and Fahmy, S., 2004, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-Hoc Sensor Networks," IEEE Trans. Mobile Computing, 3(4), pp. 366-379.

[8] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., 2006, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Trans. Dependable and Secure Computing, 3(1), pp. 62-77.

[9] Shehab, M., Bertino, E., and Ghafoor, A., 2005, "Efficient Hierarchical Key Generation and Key Diffusion for Sensor Networks," Proc. Second Ann. IEEE Conf. Sensor and Ad Hoc Comm. and Networks, pp. 197-213.

[10] Ganeriwal, S., Balzano, L. K., and Srivastava, M. B., 2008, "Reputation-Based Framework for High Integrity Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, pp. 66-67.

[11] Boukerch, A., Xu, L., and El-Khatib, K., 2007, "Trust-Based Security for Wireless Ad Hoc and Sensor Networks," Computer Comm., 30, pp. 2413-2427.

[12] Yao, Z., Kim, D., and Doh, Y., 2006, "PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security," Proc. Third IEEE Int'l Conf. Mobile Ad-Hoc and Sensor Systems, pp. 437-446.

[13] Liu K., Abu-Ghazaleh N., and Kang K.-D., 2007, "Location Verification and Trust Management for Resilient Geographic Routing," J. Parallel and Distributed Computing, 67(2), pp. 215-228.

[14] Chen H., Wu H., Zhou X., and Gao C., 2007, "Reputation-Based Trust in Wireless Sensor Networks," Proc. Int'l Conf. Multimedia and Ubiquitous Eng., pp. 603-607.

[15] Zhan G., Shi W., and Deng J., 2012, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Trans. Depend.Secure Comput., 9(2), pp. 184– 197.

[16] Crosby G. V., Pissinou N., and Gadze J., 2006, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks andSystems, pp. 10–22.

[17] Li, X., Zhou, F., and Du, J., 2013, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks", IEEE transactions on information forensics and security, 8(6), pp.924-935.