Journal of Computer Science

Original Research Paper

A Novel Unique Node Based Clustering and Location-Key Pair Based Security for Wireless Networks

[1]T.R. Vedhavathy and [2]M.S.K. Manikandan

[1]*Department of CSE, KLN College of Engineering, Sivagangai, India*
[2]*Department of ECE, Thiagarajar College of Engineering, Madurai, India*

Article history
Received: 12-04-2014
Revised: 23-04-2014
Accepted: 24-03-2015

Corresponding Author:
T.R. Vedhavathy
Department of CSE, KLN College of Engineering,
Sivagangai, India
Email: trveda@gmail.com

Abstract: Wireless ad hoc networks are used in emergency situations especially for surveillance and monitoring. The nodes in the ad hoc networks are self-organized and can accommodate by themselves with the available resources. The nodes are capable of random movement and hence there is no fixed infrastructure. The purpose of the ad hoc networks can be fulfilled only if all nodes cooperate in routing for successful delivery of packets. But in practice, some nodes may become malicious so as to preserve their own resources. If the number of such malicious nodes increases, the performance of the network degrades significantly. In this study we introduce a novel unique node based clustering and location key pair based security for the detection of malicious nodes in the network. The simulation results show that the proposed approach is more efficient in the detection of malicious nodes.

Keywords: Wireless Ad Hoc Network, Novel Clustering, Security, Key-Pair, Malicious Nodes

Introduction

Wireless ad hoc network is a collection of mobile nodes that can communicate with each other via wireless links. The nodes are self organized in nature and don't have a fixed infrastructure. The network topology changes dynamically due to the movement of the nodes. The nodes individually or collectively perform routing and data forwarding themselves. The resource consumption of the nodes vary based on the application of the network.

The current routing protocols for MANETs are based on the assumption that all the nodes cooperate in routing and data forwarding. But this is not the case in practice. Due to the availability of low resources like computing power, battery life and energy, some nodes may behave maliciously in the sense that they will agree on routing but don't perform data forwarding for other nodes as it will consume their valuable resources. The malicious nodes are willing to spend their resources only for themselves i.e., to forward their own packets. Such nodes won't spend their resources for forwarding others' packets; they won't forward the packets meant for other nodes; they simply drop the packets of other nodes.

If the percentage of such malicious nodes increases, the performance of the network degrades significantly and hence the purpose of the network fails (Hatware *et al*., 2012; Miranda and Rodrigues, 2002; Marti *et al*., 2002). Therefore it is necessary to monitor the nodes joining or leaving any area of the network as well as the nodes currently available in the coverage area of the network to determine whether the nodes are trusted nodes or malicious nodes. Various intrusion detection/prevention mechanisms are applied to detect the malicious nodes and clustering methods are used to minimize the energy consumption.

In this study, Novel Unique Node Based Clustering (NUNBC) technique is used to reduce the energy consumption of nodes and location key pair is used to detect the malicious nodes so as to improve the security of the network.

Related Works

Numerous methods have been projected to detect or prevent malicious activity in wireless networks. Given below are the synopses of a few papers presented:

Liu *et al*. (2007; Chobe and Gothawal, 2013), the author proposed the 2ACK scheme that helps as an add-on method for routing systems to sense routing misbehavior and to alleviate their opposing effect. The key impression of the 2ACK scheme is to send two-hop response packets in the reverse direction of the routing path. In order to decrease extra routing overhead, only a

portion of the received data packets are acknowledged in the 2ACK scheme.

The idea of nugglets is used as payment in (Jakobsson *et al*., 2003). There are two prototypes1) Packet trade type 2) Packet purse type. In the Packet Trade type, each in-between node purchases the packet from the earlier node for some nugglets and retails it to the following node for more nugglets.

Marti *et al*. (2002), the watchdog and the path rater mechanism is used to detect and eliminate the malicious nodes. The Best-effort Fault-Tolerant Routing (BFTR) system also employs end-to-end ACKs (Xue and Nahrstedt, 2004). Khatawkar *et al*. (2011), various systems were discussed that serve as an add-on technique to detect routing misbehavior and to mitigate their adverse effects. But applying monitoring mechanism to validate each individual node in the route brings more effect than other techniques. (Manjula and Chellappan, 2012) proposes a technique called Randomized and Trust based watcher judgment strategy for duplication attack detection mechanisms in wireless networks (RTRADP) using trust factor.

Bhattacharjee *et al*. (2013) proposed a novel mechanism to verify the neighbor nodes and select a secured shortest path to transfer the data in secured manner. Shan *et al*. (2013), the author analyses the energy economy by LEACH protocol in various kinds of WSN. The necessity for safety in LEACH protocol has motivated many scholars to design protected versions of this protocol and to create it resilient against insider and outsider attacks. Masdari *et al*. (2013), the author discussed about the current state-of-the- art secure LEACH schemes that are proposed in literature. In (Sarma *et al*., 2011), a novel secure routing protocol is projected for wireless sensor networks in which sensor nodes as well as the base station are mobile. The protocol achieves security through symmetric key cryptography and threshold key cryptography.

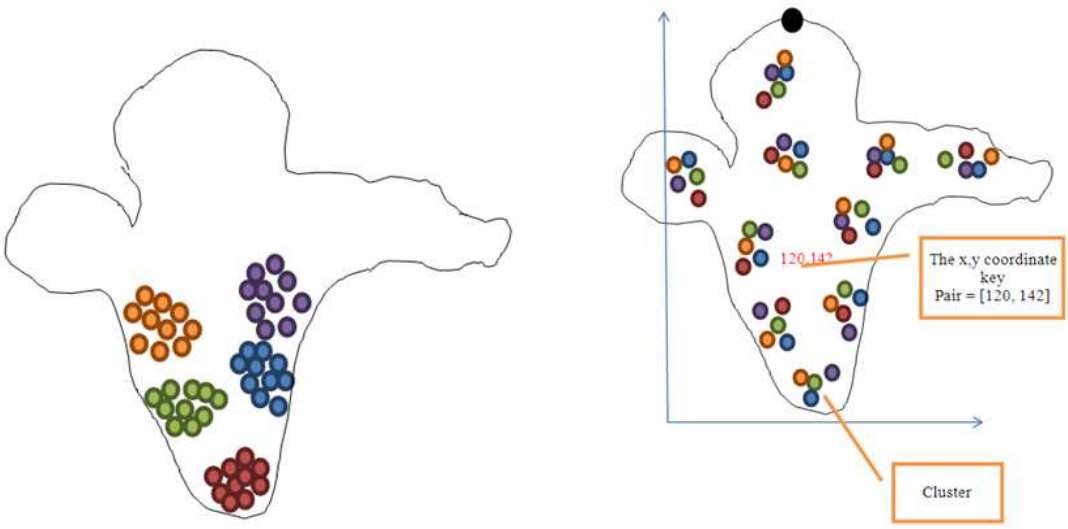
Proposed Approach

The network area is considered to be deployed in a military application. The network consists of n number of soldiers (nodes). The soldiers (nodes) are selected from different states (categories). A constant k is defined to form the number of clusters [groups] in the network. Each cluster contains k number of nodes by carefully placing the nodes from each category. The clusters are formed in such a way that each cluster has at least one node from each category and so each cluster contains all categories of nodes. The placement of nodes before and after clustering is shown in Fig. 1a and b.

For example, if there are 10 states, 10 soldiers are selected from each state to have a total of 100 soldiers. These soldiers are grouped into 10 clusters such that each cluster has 10 nodes from each state. The nodes are placed in a random location [x, y] within the cluster area and this location value is assigned as the key to that particular node as per Equation (1). Figure1 shows the cluster formation and the key assignment to nodes as per their location:

$$key\ (node_i) = node_i\ (x_i\ ,y_i) \quad (1)$$

For data communication, a node is required to submit its key pair; if the key value is valid, the node is allowed to communicate with other nodes, otherwise the node is blocked from communication.



(a) (b)

Fig.1. (a) Placement of nodes before clustering. (b) Placement of nodes after clustering

Algorithm

Network G = {N_1 ,N_2,.. ….N_M} ∀N_i ∈

N is the Number of Nodes in the network G

Define K where k =

$\frac{N}{K}$ *, K is number of clusters, k is a constant*

for j = 1 *to M*

for i = 1 *to k*

if (*Ni ! = Nj*) *then*

ci (*Ni*) = *add* (*Ci, Nodei*)

End if
next i
next j
For I = 1 to k
Key (*Ni*) = *Ni* (*x, y*)
next i
for i 1 to M
for j = 1 to k
if (*Ni. x, Ni. y ==key* (*Ni*) *then*
Ni → *message to BS*
Update Energy (*Ni*)
End if
Next j
Next i
for i = 1 to k
CHi = max (*max*((*energy*(*Ni*)))
Next i
for j = 1 to M
for i =1 to k
CHi ←
aggregate Data (*CHi. data, Ni. data*)
next i, j
for I = 1 to k
BS ← *CHi.Aggregated DAta*
Next i
end

The network G contains the M number of nodes [N] and each node has its own characteristics like energy, base location and current location [x, y]. To save the energy, the NUNBC technique is used for clustering the nodes. It is assumed that the nodes are from different states and they are placed in the Head Location of a country. The number of nodes taken from each state is the number of clusters or the number of clusters in the network is the number of nodes taken from each state. It means that each cluster should have at least one node from each state, all the nodes in a cluster belongs to all the states.

When the number of nodes in the network increases gradually, they are added one by one in each cluster in equal manner. Once it reaches the maximum limitation of the cluster size, a new cluster will be formed.

When a node is initialized or placed in a cluster at (x, y) location, this x and y value is assigned as the private key and public key respectively to that particular node. When a node is initialized and clustered, each node should send a HELLO message to the Base Station after its key pair value is validated. Based on the distance and message size, all the nodes lose some energy. According to the energy value, the node with the highest energy level is elected as CH in each cluster. The cluster nodes communicate to the base station with the help of the CH and the CHs gather and aggregate the data to the BS. The CH election process is executed regularly in the network at periodic time intervals.

The NUNBC technique allows only the trusted nodes in the network to communicate with each other. The malicious nodes or the nodes with invalid key pair value are detected and blocked from communication. The proposed technique also achieves energy saving and allows only the trusted nodes for communication.

Simulation Settings

The proposed algorithm is coded in Network simulator 2 and the performance of the proposed approach is verified. In the NS2, the size of the network is assumed as 1200 × 1200 and 100 number of nodes deployed in the network and clustered. There are 10 clusters where each cluster contains 10 nodes and each node belongs to one state, totally 10 states. The parameters of the nodes and the channel characteristics assigned in the TCL code are given in the following table. NS2 version 2-3.4 has been used to analyze the proposed approach with the routing protocol AODV. The under lying MAC protocol defined by IEEE 802.11 is used Traffic sources of both Continuous Bit Rate (CBR) based on TCP for 10 sources are generated. The CBR and TCP mobility scenario of 20 nodes with a maximum speed of 30 sec. for a simulation area of 1200×1200 with 2.0 Mbps was generated.

Table 1. Simulation system parameters

Parameter	Value
X, Y	1200, 1200
Routing protocol	AODV
PROB	Radio propagation
NN	100
MAC	MAC/802.11
Energy model	Energy-model = true
Mobility	Random
Moving speed	2 m/s
Traffic	CBR
Bandwidth link	2 Mbps
Propagation path loss model	Two-Ray ground model

DOI: 10.3844/jcssp.2015.534.539

Results

Simulation with Various Number of Nodes

The misbehavior of the malicious nodes in the network is incorporated as the same as done in (Manjula and Chellappan, 2012). The proposed approach is implemented in TCL with various numbers of nodes deployed in the network like 25, 50, 75 and 100 nodes.

The malicious nodes are detected according to the authentication verification. The performance of the network is evaluated with the main factors like the number of malicious nodes detected, throughput and energy.

Figure 2 shows the detection of malicious nodes before and after the deployment of the proposed Approach. Figure 3 shows the energy consumption of the nodes before and after the deployment of the proposed approach and Fig. 4 shows the throughput of the network before and after the deployment of the proposed approach.

Discussion

The misbehavior node is detected only by verifying the key pair which means if and only if the node belongs to the particular cluster and in the particular network region, it is allowed for communication. According to the number of nodes in each simulation round, the result is generated and given in graph form for analyzing the performance.

During simulation the important factors of the network like energy, malicious node detection rate and the throughput are captured from the trace file generated automatically and plot as a graph.

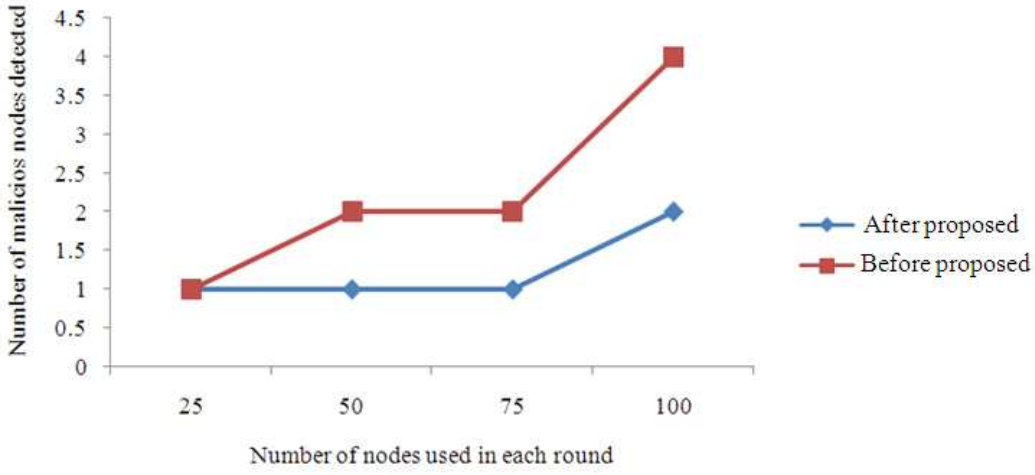


Fig. 2. Malicious node detection before and after deployment of proposed approach

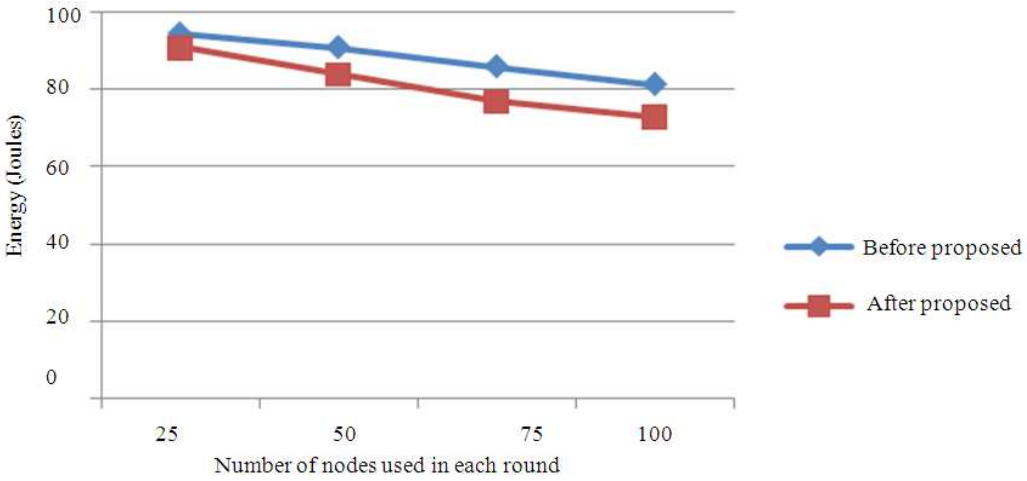


Fig. 3. Energy consumption before and after deployment of proposed approach

DOI: 10.3844/jcssp.2015.534.539

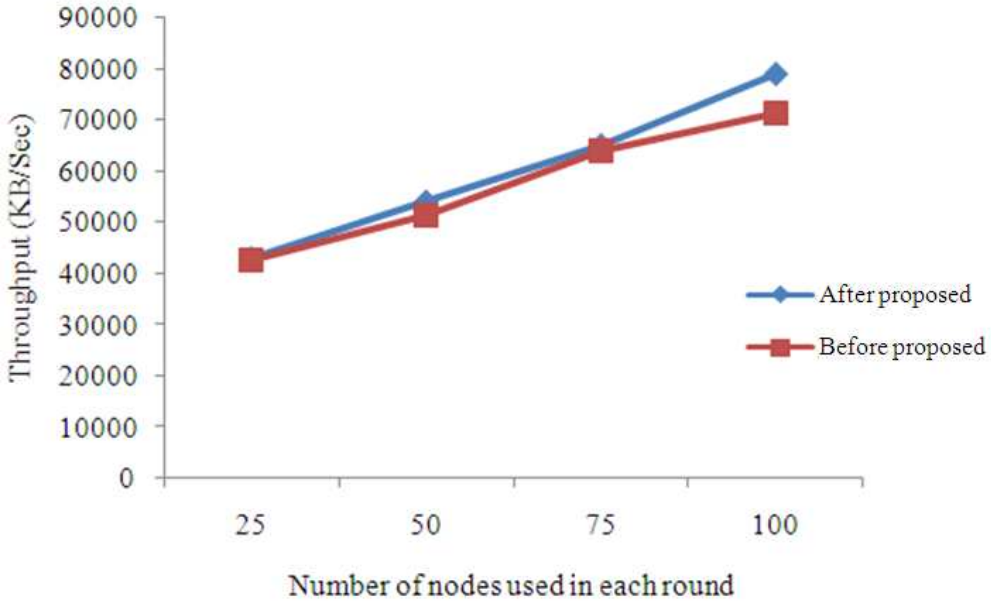


Fig. 4. Throughput obtained before and after deployment of proposed approach

In Fig. 2, the number of malicious nodes detected by the proposed approach is less since the malicious activity is reduced in the proposed approach during the initialization of the network itself. Even though some less number of nodes tried from outside the network to act as malicious, they are detected accurately by the proposed approach and the detection rate is shown in Fig. 2 clearly.

In case of energy saving the proposed approach results in less energy consumption by the nodes and it is clearly depicted in Fig. 3. The proposed approach retains 94.58, 91, 86 and 81.34% of the energy in all the four rounds with 25, 50, 75 and 100 nodes respectively whereas before deployment, the system retains 91%, 84%, 77% and 73% of the energy in all the four rounds with 25, 50, 75 and 100 nodes respectively.

In terms of throughput the proposed approach obtained more successful transmission in the network and it is clearly depicted in Fig. 4. The proposed approach transmitted 43000, 54000, 65000 and 78900 packets in all the four rounds with 25, 50, 75 and 100 nodes respectively whereas the system transmitted 42500, 51345, 63749 and 71234 packets in all the four rounds with 25, 50, 75 and 100 nodes respectively without the proposed technique.

Conclusion

In the proposed approach, the clustering mechanism is used to reduce energy consumption of the network nodes and hence to increase the network life time. The unique location key which cannot be modified or duplicated by any other node provides high security to all the nodes in the network. Hence NUNBC technique provides more reliable and better performance in detecting the malicious nodes so that they can be avoided while making routing decisions. It is concluded that the proposed approach results in better performance of the network in terms of detection rate, energy and throughput.

NUNBC concentrates only on node level security and it can be further improved by including data level security in the network. The efficacy of the data level security can be improved by applying an efficient data encryption-decryption algorithm.

Funding Information

The authors have no support or funding to report.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Jakobsson, M., J.P. Hubaux and L. Buttyán, 2003. A micro-payment scheme encouraging collaboration in multi-hop cellular networks. Proceedings of the 7th International Conference on Financial Cryptography, Jan. 27-30, Springer, West Indies, pp: 15-33. DOI: 10.1007/978-3-540-45126-6_2

Bhattacharjee, S. 2013. Distributed algorithm for dynamic data-gathering in sensor network. Cornell University.

Chobe, S.N. and D. Gothawal, 2013. An acknowledgement based approach for routing misbehavior detection in MANET with AOMDV. Int. J. Adv. Comput. Eng. Network., 1: 5-10.

Hatware, I.V., A.B. Kathole and M.D. Bompilwar, 2012. Detection of misbehaving nodes in Ad hoc routing. Int. J. Emerging Technolo. Adv. Eng., 2: 6-11.

Khatawkar, S.D., U.L. Kulkarni and K.K. Pandyaji, 2011. Detection of Routing Misbehavior in MANETs. 1st Edn., IACSIT Press, Singapore.

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mobile Comput., 6: 536-550. DOI: 10.1109/TMC.2007.1036

Manjula, V. and C. Chellappan, 2012. Trust based node replication attack detection protocol for wireless sensor networks. J. Comp. Sci., 8: 1880-1888. DOI: 10.3844/jcssp.2012.1880.1888

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2002. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th annual international conference on Mobile computing and networking, Aug. 06-11, Boston, MA., USA, pp: 255-265. DOI: 10.1145/345910.345955

Masdari, M., S.M. Bazarchi and M. Bidaki, 2013. analysis of secure leach-based clustering protocols in wireless sensor networks. J. Netw. Comp. Appli., 36: 1243-1260. DOI: 10.1016/j.jnca.2012.12.017

Miranda, H. and L. Rodrigues, 2002. Preventing selfishness in open mobile ad hoc networks.

Sarma, A.H.K.D., B.A. Kar and C.R. Mall, 2011. Secure routing protocol for mobile wireless sensor network. Proceedings of the IEEE Sensors Applications Symposium, Feb. 22-24, IEEE Xplore press, San Antonio, TX, pp: 93-99. DOI: 10.1109/SAS.2011.5739778

Shan, J., L. Dong, X. Liao, L. Shao and Z. Gao *et al*., 2013. Research on improved LEACH protocol of wireless sensor networks. Beijing Institute of Technology.

Xue, Y. and K. Nahrstedt, 2004. Providing fault-tolerant ad hoc routing service in adversarial environments. J. Wireless Personal Communi., 29: 367-388. DOI: 10.1023/B:WIRE.0000047071.75971.cd