 ISSN: 2321-8169
1768 – 1772

Clone Detection for Efficient System in Wireless Sensor Network Using Ad Hoc on Demand Distance Vector (AODVC)

Submitted By
Ms. Rupika Yadav
M Tech III Sem
TGPCET, Nagpur

Co-guide
Prof Vishal Tiwari
Dept. of CSE
TGPCET, Nagpur

Guide
Prof Roshani Talmale
HOD, CSE
TGPCET, Nagpur

Abstract— Energy and memory efficient for clone detection protocol in deployed WSNs, which can maximize the chances of successful clone attack detection and maintain adequate network lifetime. Specifically, we utilize the location information of sensors and randomly select witness nodes located in a ring area to verify the privacy of sensors and to detect clone attacks. The ring structure provides energy and memory efficient data flowing along the path towards the witnesses and the sink. Here we theoretically prove that the proposed protocol can achieve maximum percent clone detection probability with trustful witnesses. **A***d Hoc* **O***n-Demand* **D***istance* **V***ector* (AODV) a routing protocol for ad hoc mobile networks with large numbers of mobile nodes. The protocol's algorithm creates routes between nodes only when the routes are requested by the source nodes, giving the network the flexibility to allow nodes to enter and leave the network at will. Extensive simulations illustrate that our proposed protocol can accomplish long network lifetime by effectively distributing the traffic load across the network.

Keywords— *Security attack, Base Station, Clone attack, Clone attack detection, Centralized approach, Distributed approach.*

*****

I. Introduction

To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection.

Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM) use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs.

In the proposed protocol, initially nodes send claiming messages containing its neighbor list along with a maximum hop limit to randomly selected neighbors; then, the sequent message transmission is regulated by a probabilistic directed technique to approximately maintain a line property through the network as well as to incur sufficient randomness for better performance on communication and resilience against adversary. In advance, border determination mechanism is employed to further reduce communication payload. While forwarding, intermediate nodes explore claiming messages for node clone detection. By proposal, this protocol consumes almost minimal memory, and the proposed method simulations show that it outperforms all other detection protocols in terms of communication performance, while the detection probability is satisfactory.

1.1 Background of Present Work:

Wireless sensor network is a fusion of sensor nodes and base station also known as data collection unit. Sensor nodes in WSN's are thus responsible for performing the basic functions to provide better interaction between network and real time applications. Wireless Sensor network is having number of sensor nodes which concurrently send sensed data to base station. The base station can be referred as sink node.

Once deployed, nodes have the capability to self-configure using a discovery protocol and form neighbourhood's. Node communication from sink or base station to each node is determined by the routing strategy in place. Reliable routing is crucial to the success of WSNs where up to the minute data is required for many applications. While there has been a significant amount of research into this topic, determining the best protocols to be used in any situation require testing of the environment that a node will be in. Testing on the actual environment however is not a feasible option due to monetary and time constraints.

 ISSN: 2321-8169
1768 – 1772

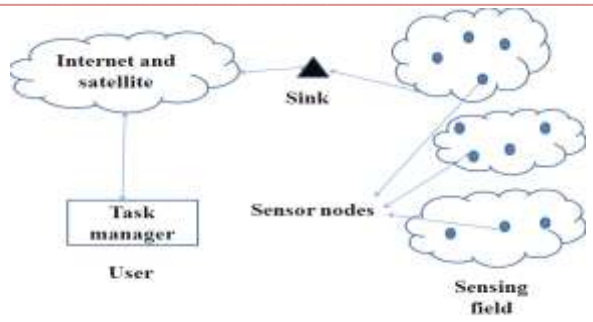

Figure 1.1: Wireless sensor network

Figure 1.1 shows the general scenario of wireless sensor network represents sensor nodes with base station. Sensor nodes are deployed in sensing field which is responsible for sensing the required information or data and pass it to the base station via a desired path, from where data can be transfer to the multiple users for processing.

Based on this specification data can be sent from source node to sink node either dynamically or statically. The network can be heterogeneous network or homogeneous network. Depending on the scenario, the necessity of continuous monitoring i.e. information need to send to sink node continuously. The applications such as in area and industrial monitoring, health care monitoring, military application, forest fire detection requires continuous monitoring.

1.1.1 Components of sensor node

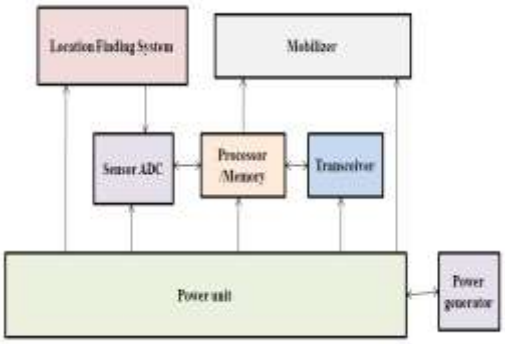

Figure 1.2: Sensor node's Components

As shown in above figure 1.2 the nodes are embedded in a particular device having variety of components viz. power source, positioning system, sensing unit, mobilizer, memory and processing unit. Sensor nodes are having limited energy or battery sources. For prolonging the lifetime of network and to make use of limited available battery source care has to be taken as replacement of battery power is impractical.

1.1.2 INITIAL NODE CONFIGURATION

Wireless Sensor Networks (WSN) are very uncharacteristic of other networks. Initial configuration of a network is not done manually like is the case with current computer networks; WSN nodes are capable of self-configuring in order to form a reliable network. Unlike other types of networks, a node does not need to connect to a router directly, it can use other nodes to connect and pass messages while interacting with the environment; this is typical of ad-hoc networks. When a node is initially deployed, the first step that is performed to configure the network is to determine each node's neighbouring node and identify a possible link through the use of a connection or neighbourhood table. The table serves as a means of not only routing messages but also aids in maintaining the network.

Node discovery is not limited to the initial node deployment; discovery can also take place when new nodes join an existing network or when node failure occurs. Discovery can take place through various Hello Protocols in which a node transmits a "Hello" packet and listens for a reply. If an acknowledgement is received a node will then add the acknowledging node to its connection table. One of the more prominent, and simplistic protocols that are currently being used is that of the Basic Hello Protocol. In this protocol, a node can be in one of two states; talking or listening. The two states occur within a time frame *w* of duration *f*, as illustrated in Figure 1.3.

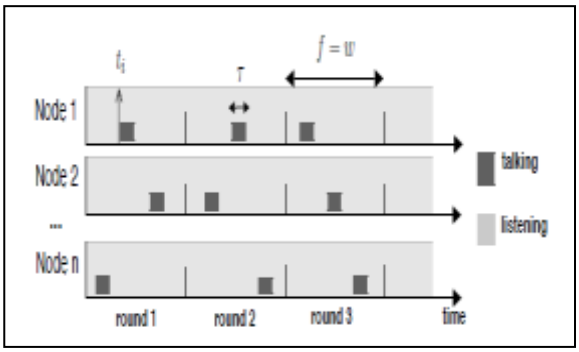

Figure 1.3. Basic Hello Protocol

A different version of the Basic Hello protocol is that of the Energy Aware Hello Protocol which incorporates three different states; talking, listening and sleeping. As seen in Figure 1.4, the protocol addresses the power constraint by entering a sleep state during periods of inactivity. During this time the node will turn the radio interface off and is unable to communicate with the other nodes.

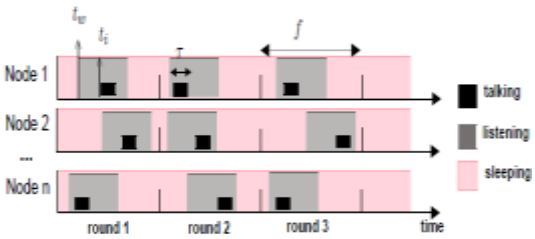

Figure 1.4. Energy Aware Hello Protocol

 ISSN: 2321-8169
1768 – 1772

Both Basic and Energy Aware Hello Protocols represent two different ways of successfully achieving node discovery. Both protocols have trade-offs and depending on the purpose and intended duration of a WSN one protocol might prove better use over the other.

1.1.3 ROUTING STRATEGIES

Routing within a WSN is very different from routing in traditional computer network. WSN are dynamic in nature, they can be in various stages at any given time and may not always have the same neighbours or be in the same location. Existing strategies such as TCP/IP routing cannot be employed, rather new routing strategies are implemented.

I. One Hop Routing: Perhaps one of the simplest way to achieve routing is to use a centralized node to route messages through the network as seen in Figure 1.5. This strategy, known as One-Hop Routing is simple to implement, however it is only feasible under certain conditions such as a small contained WSN.

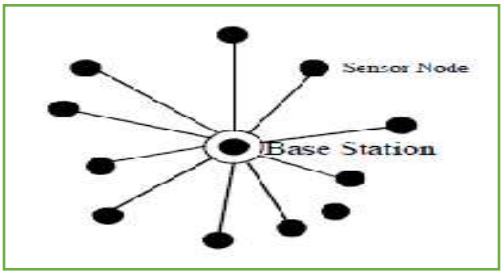

Figure 1.5: One Hop Routing Strategy

II.Multi Hop Routing: A different type of routing strategy that enjoys success with WSN is that of multi-hop routing. Under this model a node will forward a packet to one of its neighbours and in turn the neighbour will forward the packet to its neighbours as seen in Figure 1.6. The process is repeated until the sink or a base station is reached.

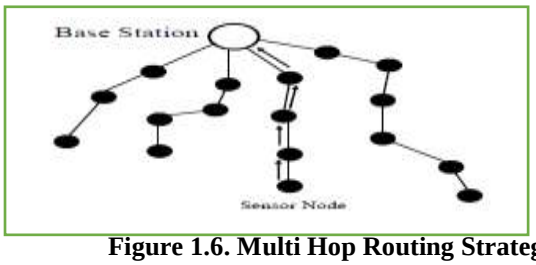

Figure 1.6. Multi Hop Routing Strategy

III. Cluster Based Routing: One of the goals of any routing strategy is to make a network as useful and efficient as possible. Under a cluster based routing strategy, different nodes form groups in order to efficiently relay data to the sink or base station. For every cluster there is a cluster head. These nodes perform aggregation and are able to send a coherent packet that reflects the data sensed by the cluster to the base station. Figure 1.7 demonstrates such type of network, where the nodes join a cluster head to form a sub network using a one-hop routing. The cluster heads in turn form a separate network that is able to communicate with the base station through multi-hop routing.

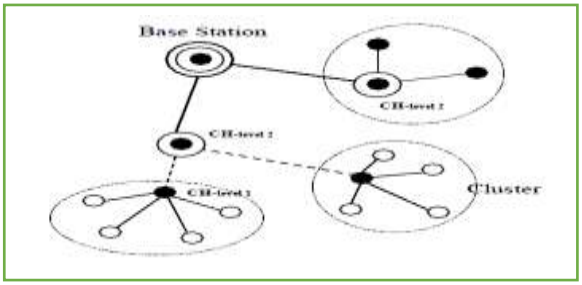

Figure 1.7. Cluster-based Hierarchical Routing Strategy

1.1.4 Mobile sink

In WSNs the strategy to be used depends on the application for which it is deployed. In some applications nodes can be deployed in a predefined manner and the route will be static. Whereas in some other applications random deployments are needed, routes have to be decided dynamically.

But due to converge-cast traffic scenario in static network topology the overhead on base station increases as it must active all time in order to transmit data between sensor nodes hence increases energy consumption. To resolve this issue mobility of sink can done. As shown in figure 1.8 mobile sink collect data by traveling throughout the network.

Using mobile sink in wireless sensor network data transmission can be done very fast, reducing energy consumption and prolong the network lifetime. The mobility of base station can be classified in either random based mobility or controlled based mobility.

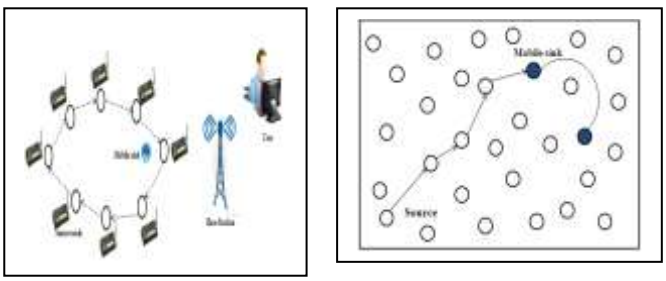

Figure 1.8: Mobile sink in wireless sensor network

1.1.4.1 Random based mobility

In random based mobility information about network is not requires as there is not intercommunication on regular basis. Mobile node collects data from nodes only if it is in within rage. The performance of network degraded as there is continuous monitoring of base station and dynamic route rearrangement.

1.1.4.2 Controlled based mobility

Whereas in controlled based mobility the movements of mobile sink are not deterministic. Controlling the parameters of networks such as residual energy level of sensor nodes over data path, event occurring in particular area, different trajectories of mobile entities and velocity efficient utilization of energy can be increased. Also if required the mobile nodes are informed to gather data within specified time interval.

II. Motivation*:*

A sensor node deployed unattended in an insecure environment such as in enemy territory or in a dense forest, is prone to serious threats like node replication attack. Sensor nodes that are deployed in hostile environments are vulnerable to capture and compromise. An adversary may obtain private information from these sensors, clone and intelligently deploy them in the network to launch a variety of insider attacks. This attack process is broadly termed as a clone attack. Currently, the defenses against clone attacks are not only very few, but also suffer from selective interruption of detection and high overhead (computation and memory).

Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors. To prolong the network lifetime, i.e., the time duration from the start of network until the first occurrence of a sensor that runs out of energy, it is critical to not only minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas of WSNs.

Some distributed clone detection protocols have been proposed, such as Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM). In most existing clone detection protocols, the required buffer storage size depends on the network node density, i.e., sensors need a large buffer to record the exchanged information among sensors in a high-density WSN, and thus the required buffer size scales with the network node density.

Such requirement makes the existing protocols not so suitable for densely deployed WSNs. A wireless ad-hoc network, also known as IBSS Independent Basic Service Set, is a computer network in which the communication links are wireless. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts. A major limitation with mobile nodes is that they have high mobility, causing links to be frequently broken and reestablished. Moreover, the bandwidth of a wireless channel is also limited, and nodes operate on limited battery power, which will eventually be exhausted. Therefore, the design of a mobile ad hoc network is highly challenging, but this technology has high prospects to be able to manage communication protocols of the future.

Most approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy consumption in WSNs. Some sensors may use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs. Most existing approaches can improve the successful clone detection at the expense of energy consumption and memory storage, which may not be suitable for some sensor networks with limited energy resource and memory storage.

This motivates to design an efficient clone detection mechanism having higher detection probability, lower detection time, lower false positive, and lower communication and storage overhead. For we propose a new effective and efficient scheme to detect such clone attacks.

III. *Scope of Present Work*

To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection.

Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM) use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs.

IV. Objective

Improve performance: The performance of the ERCD protocol is evaluated in terms of clone detection probability, power consumption, network lifetime, and data buffer capacity.

Extensive simulation: Extensive simulation results demonstrate that our proposed ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.

Experiment results: The experiment results demonstrate that the clone detection probability can closely approach maximum percent with untrustful witnesses.

Energy consumption: By using ERCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.

V. Problem Definition

Detection of Malicious Nodes: Is to make it difficult for malicious users the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages.

Existing system : The existing system does not make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not.

Probabilistic approach of cloning: Does not guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design.

Design criteria: The design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors.

Sensor: It minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas of WSNs.

Acknowledgments

The authors wish to thank Dr. Yingpei Zeng, Dr Shigeng Zhang of State Key Laboratory for Novel Software Technology, Nanjing University, China, for providing us technical details and simulation code. The authors also like to thank Prof Yang Xiang and Dr T H Luan of School of Information Technology, Deakin University, Australia for their valuable suggestions to in improve our idea. The authors wish to acknowledge the anonymous reviewers for their valuable comments.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[4] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7,pp. 1036–1045, Sep. 2010.

[6] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[7] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

[9] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[10] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[11] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks,"IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.