Energy Efficient and Reliable Algorithm to Detect and Resolve Sinkhole Attack over Collection Tree Protocol

Maya Shelke
Assistant Professor,
Department of CS and IT,
Symbiosis Institute of Technology(SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

Kalyani Kadam
Assistant Professor,
Department of CS and IT,
Symbiosis Institute of Technology(SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

Ameya Bhattacharya
UG Student,
Department of Computer science,
Symbiosis Institute of Technology (SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

Richita Das
UG Student,
Department of Computer science,
Symbiosis Institute of Technology (SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

Ayushi Rathi
UG Student,
Department of Computer science,
Symbiosis Institute of Technology (SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

Aishwarya Singh
UG Students,
Department of Computer science,
Symbiosis Institute of Technology (SIT),
Pune, Affiliated to Symbiosis International University (SIU), Pune, Maharashtra, India.

ABSTRACT
Wireless sensor networks (WSNs) have gained huge popularity in various new fields. The direct use of each of these sensors individually is to detect its surrounding conditions such as temperature, pressure, sound, motion etc. whereas a collection of such nodes finds application in various large scale management systems such as healthcare, disaster and traffic management programs. In most of these systems, the sensors are located at points which are not physically protected and can hence fall prey to several security threats and attacks very easily. The limited memory, power and capacity of such sensors make it more difficult to introduce advanced, heavy-weight algorithms for securing them against such attacks. Further, the criticality of the applications using WSN makes such security threats more dangerous. In this paper, we show the results of combining a novel detection algorithm with the results of a unique resolution technique of the sinkhole attack when the network is routed using Collection Tree Protocol (CTP).

General Terms
Security, Algorithm, Attacks

Keywords
Wireless Sensor Network (WSN), Collection Tree Protocol (CTP), Sinkhole Attack, Base Station (BS), Cluster Head (CH), Sensor, Internet of Things (IoT)

1. INTRODUCTION
Wireless sensor networks (WSNs) are made up of a large number of heterogeneous sensor nodes distributed across geographical areas of different scales, depending upon the application. The nodes are used to sense various types of data depending on the application's functionality .The sensors being deployed are constricted in many aspects such as their memory capacity, battery life and their computational powers. The nodes are allocated a unique key by using various techniques to bind them to the particular network [2]. They sense the required data and forward the collective data to their base station (BS) for storage or further computations and there are numerous existing routing protocols of path resolution to realize the same. WSNs are used in a variety of fields like defense, Intelligent Transport System (ITS), smart homes, Health Care Management System, to name a few. In all of the above mentioned applications, it is imperative that the WSN nodes function accurately and efficiently. All the same, considering the constraints imposed on the WSN sensor nodes, it is not possible to implement a strong security technique in the sensors without it taking a toll on the sensor resources. Therefore, the security of the nodes is an area which has to be sacrificed most of the times to optimize the lives of the other resources of the nodes. Hence, the WSNs haven't yet been exploited to their full capacities in any project. Nevertheless, in some of the above mentioned areas, like Health Care, it is indispensable that the data be authentic and secure.

To demonstrate the criticality, we present the example a Health Care Management System. Use of the Internet of Things (IoT) in this sector could save an estimated amount of $63 billion in over 15 years with a 15 to 30 percent reduction in hospital equipment costs and a 15 to 20 percent increase in patient throughput [3]. Nevertheless, this profit is negligible compared to the disaster in case of a malfunction (accidental or malicious). Cyber physical systems are essentially mechanical devices with an in-built connectivity and communication capability components. According to this report, implementation of the WSNs as a part of the medical sector would save billions of dollars however, no such plan can be conceived till the security issue of the sensors is resolved. Now, considering a scenario where a Smart

Healthcare System has been implemented, the system would require to have all the health related data for all the patients. Also, a database for all the hospitals along with the associated doctors, their specializations and the facilities provided has to be maintained. In case of a medical emergency, the system should be capable of diagnosing the crisis, assessing all the hospitals in the nearby locality, deciding which hospital is best capable of handling the situation and accordingly informing the concerned hospital. Additionally, the system has to resend the call signal to the hospital if no help arrives within the stipulated time lapse along with a demand for the status of help. If no acknowledgement is received, the system has to assume that the hospital will not be able to cater to the situation and send a help signal to the next nearest hospital. Simultaneously, it also has to continuously monitor the patient's condition and keep on sending the latest health status updates to the hospital along with the signal. In this whole system, there are numerous sensor nodes involved. The basic flow of the signal can be described as: from sensor at patient's house to the cluster head (CH) or parent node, from CH to the BS and from the BS to the chosen hospital. These will be the landmark sensors along with a plethora of intermediate nodes. If anyone of the intermediate node is a victim to the hacker's attack, all the critical data may be available to the hacker at his disposal. The signal might not be forwarded at all or tampered or incomplete data might be sent. Here, any of the above might lead to the death of the patient in question. From the above example, the need for the node's security is evident. The various types of attacks the system might fall prey to include sinkhole attack, blackhole attack, selective forwarding, tampering, wormhole attack. Out of all the attacks, we focus on the sinkhole attack. Sinkhole attack is a network layer attack and the threat posed by it is the worst compared to the other types of attacks [4]. In a sinkhole attack, the main objective is to attract all the flow of data in the network towards the affected node. This is achieved by either pretending that the malicious node has a higher link quality network path to the base station or by downplaying the network links of the other nodes. Sinkhole attacks are extremely potent as they lay foundation to many more attacks If a system falls prey to this attack, the attacker could drain all the available data on the network, forward a selective set of information while keeping back the major chunk (selective forwarding attack) or forward edited data which may convey a misleading representation of the data. Therefore, the system actually becomes vulnerable to multiple attacks all at once. Also, a sinkhole attack is exceedingly simple to launch in a WSN. The attacker lies listening for update messages sent to the target by its neighbors. He can then alter the message and replay it later pretending to be the original sensor. In our paper, we have chosen the underlying routing protocol to be Collection Tree Protocol (CTP). It is a type of tree based protocol implemented on TinyOS. It is a multi-hop routing protocol with a 90% successful data transmissions rate making this protocol highly efficient [5]. It is an address free protocol which essentially means that the nodes have no permanent identifier pointing to them. CTP can be fashioned differently to suit different applications. Regardless CTP consists of three components which are the Routing Engine (RE), Forwarding Engine (FE) and Link Evaluation Engine (LE). The RE periodically sends its routing information so that the BS can construct and sustain the routing tree. Before transmission of data, FE accesses the routing tables to decide upon best possible parent node depending on the data link quality of the nodes. The LE ensures proper maintenance and frequent revision of the link table. Every node chooses a parent node to forward the information based on the nodes' Expected Transmissions (ETX). This value indicates the energy cost involved in forwarding the data to that node hence a node chooses the node with the minimum ETX as its parent node. There is only one CH to which all the data is sent and from there the data is forwarded to the BS. The in-built process for electing the CH is random which requires minimum amount of computation and hence the process of CH change is completed within a matter of few seconds. As soon as a node becomes the CH, it advertises its ETX as 0 and hence attracts all the traffic towards itself. The CTP can be configured such that it chooses the BS based on various parameters such as the sensor network link quality or the distance. We endeavor to present a novel idea for the detection of the sinkhole attack on such a system and a way of resolving the attack.

2. RELATED WORK

A good amount of research has been carried out in the area of detection of sinkhole attack over different routing protocols in WSNs. IoannisKrontiris et al. [6] have described their study of an efficient way to recognize a sinkhole attack with MintRoute as the underlying protocol. Anthonis Papadimitriou et al. [7] have proposed a method of forming resilience against possible sinkhole attacks, that is, the concept of prevention. However, there has been relatively less work in the domain of intrusion detection in WSNs routed using CTP. One of the pioneering studies is put forward by Feng-Jun Shang et al. [4] where different data fields such as link quality, packet loss rate, are maintained by the base station in order to compute a network topology indicating the anomaly area. The suspected nodes will form a tree-like structure and the root of this will be the best candidate for the malicious machine. A detection index is considered, which varies with respect to the application of the system, if the suspected area is larger than that limit, then it is concluded that the root of the structure is the main infected node. What is not a part of any these works is the next step of resolving the sinkhole attack once it has been successfully identified. We believe that a lot can be done about the efficiency improvement of a particular routing protocol by looking into what is done after a sinkhole attack is detected. Simply revoking security keys of a compromised node is the most common way to go about excluding that particular rogue device from the network, as put forward by various authors, including Yong Wang et al. [8]. However, this involves loss of the residual energy within the node in question. This is where our idea of conditional reconfiguration of the node in question comes in, where we aim to decide whether or not to remove the device from network based on its existing energy level and a threshold energy (Eth). A tree-based reconfiguration algorithm like the one demonstrated by Qiang Wang et al. [9] is proposed to be used within this context.

3. PROPOSED IDEA

We aim to introduce a method to detect sinkhole attack in CTP along with a novel approach to recover the node based on a certain criteria, which is Eth. A WSN system for any application will be made of a fixed number of sensors with unique keys, deployed at various geographic locations. Therefore, if each time a detected infectious node is excluded from the network, the number of nodes remaining reduces making the system less efficient and increasing the probability of data packets loss. Also, every time the sensor is revoked, it is not necessary that the sensor had utilized its full battery life extent. That energy is lost on revoking the node's key. Hence we strive to reduce this phenomenon by retrieving the viable sensors. In CTP, there is one CH and the nodes send the data

to it either directly or through an intermediate node. As mentioned above, the intermediate node or the parent node is determined based on the ETX of the nodes. As sinkhole attack generally lays foundation to further attacks, we have taken two scenarios: selective forwarding (some chosen data is forwarded by the infected node) and tampering (same or less amount of data could be forwarded by the malicious node). To detect a sinkhole attack in the first scenario, we program the child code to monitor its parent node to ensure that the packet forwarded was done and that too within a given time period. For the second scenario as well, the child node monitors the parent node to ensure that the data packet is forwarded within a given time lapse as shown in figures 1(a) and 1(b).

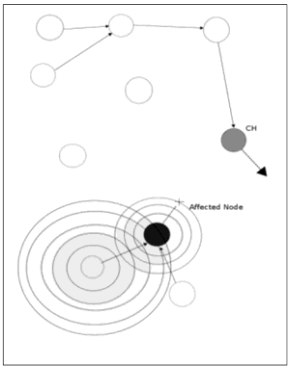

Fig.1 (a) Child monitors parent packet

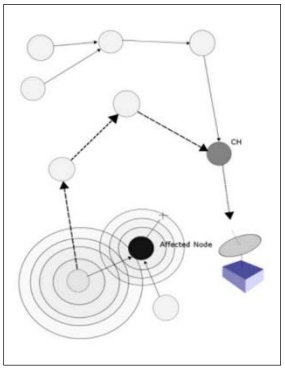

Fig.2 (b).Child re-routes packet

If the infected node is the CH itself, then the BS has to take actions to appoint a new interim CH for the remaining transaction time frame else it just checks the node's remaining battery level to decide if it is worth saving the node. Whatever course of action taken, the BS broadcasts the re-assigned values of ETX. This particular case has been represented in figure 3(a), 3(b), 3(c) and 3(d).

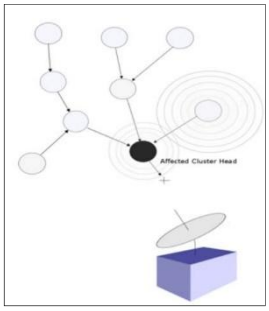

Fig. 3(a) Child monitors CH

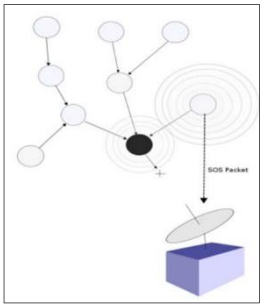

Fig. 3(b) Child sends SOS to BS

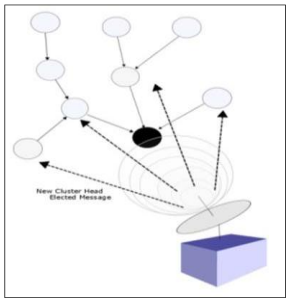

Fig.3 (c) New CH broadcast

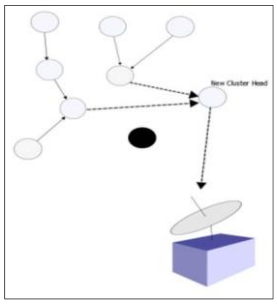

Fig.3 (d) New CH forwards to BS

The reconfiguration procedure is to restore the node to its original settings so that the link established between the node and the attacker is terminated. Generally once the compromised node is identified, the BS eliminates the node form the network. However, owing to the ease of launching a sinkhole attack, this method cannot be used to sustain a network in the long run. Neither is it feasible to physically replace all the shutdown sensor nodes. Even if new nodes are deployed they have to be connected to the BS so that the BS and the other nodes acknowledge the new node(s) as part of the original network system.

Commonly, a sensor node in CTP has a varying battery energy level depending on the kind of application or data collection it is used for. When the BS identifies the faulty node, it checks if the remaining energy level is above Eth. The value of Eth is chosen based on the different networks as the initial battery life of the node for different networks vary. If the remaining battery life is less than the Eth, the BS can just stop considering the node as a part of its system, by using the key revocation method [8] as the future productivity of the node is not worth the amount of energy required by the BS to reconfigure the node. Else, if the node's remaining energy level meets the criteria, the node is reconfigured by the BS using the code which is already available [9]. This process is to be carried out by the BS. Once the infected node is recognized and known to the BS, the BS checks the remaining resources of the sensor especially its battery life. If the remaining battery life is above a given predefined level, the BS reconfigures the sensor, effectively cutting its established link with the attacker or else the BS discontinues the use of the node. The level is determined based on the amount of energy required by the BS to reset the node. If the BS resets the nodes only to recover the node which will run out of its battery within some time, the energy exerted to accomplish the task is a waste.

4. RESULTS

We have used the NS2 simulator to simulate the algorithm proposed by us and to derive the basic result set for a set of 105 nodes in a wireless sensor network. NS2 simulator was chosen by us since most of the work in the field of wireless sensor nodes is done on this particular software and because of the strong community in case of a road block with regard to the simulator a lot solutions would be available. The documentation for the same is easily available. NS2 simulator also allows us to understand the working of a particular algorithm in terms of showing the steps in a basic visual format. We have compared our algorithm's performance with regard to that of an algorithm called Resist 1 [7] on the basis of: (a) residual energy (b) receive ratio.

A. Residual Energy

The residual energy in each node of a system which uses our algorithm (CTPS) is less than that in the corresponding node of a system which does not use our algorithm (NCTPS).

However, the technique proposed by us saves energy overall as the affected nodes in it are not always shut down, they might be reconfigured if they have energy above a threshold (considered to be 0.9 V in our simulation example).

Residual Energy (Er) = { 0, if E_r <0.9 ; E_r, if E_r >=0.9

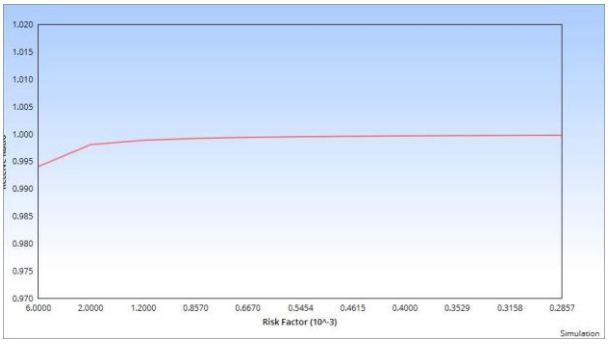

Fig. 4(b). Graph of Receive Ratio versus Risk Factor

Simulated results when plotted against each other corroborate the inverse relation. When the risk factor that is chances of a node being affected in a node is low, then the receive ratio that is probability of packets being correctly delivered to the destination is high.

5. FUTURE SCOPE

The next step is to implement the algorithm in a physical WSN where a controlled attack can be introduced in order to test it before releasing it as a final technique. It will pave the way forfuture experiments in this particular area on a large scaleIt would help make WSN systems more secure and hence be a step forward towards implementation of Internet of Things (IOT)

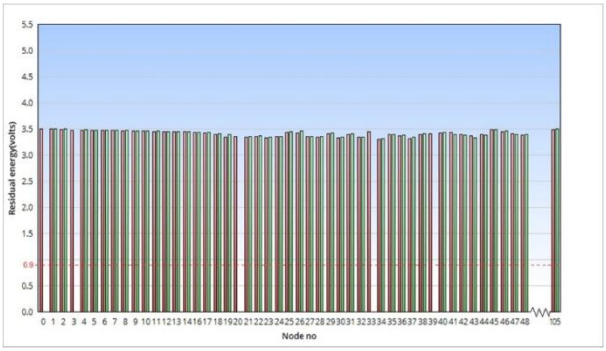

Fig. 4(a). Graph of Residual Energy per node

The graph for residual energy per node shows the levels of energy remaining in each node of the system after the simulation is over, i.e. the sinkholes have been detected and corrected, either by the proposed technique or any other algorithm of the similar kind. The graph has two series of columns, the green columns indicate the levels of residual energy per node when the proposed algorithm has been used and the red series depicts any other similar algorithm. It is clear to the reader that even though for all unaffected nodes, the residual energy is more in case of other algorithms, our proposed method results in the case where even affected nodes, if they have residual energy above a threshold, in the end contain some amount of energy as opposed to other algorithms where affected nodes are removed from the network, which is equivalent to them having 0 residual energy that can be utilized by the network.

B. Receive Ratio

Received Ratio is used to denote the ratio of the number of packets received by a node to the total number of packets sent to that node by all the other nodes.

$$P(\text{Loss}) = \frac{\text{No. of packets lost}}{\text{Total no. of packets}}$$

Receive Ratio= 1-P (Loss)

The graph for receive ratio versus risk factor indicates that there is an inverse relation between these two factors. The values of the above mentioned measures as calculated from our

6. REFERENCES

[1] Shishir Sharma and Gajendra Singh Chandel, "A Review of Pairwise of Key Establishment Techniques for Wireless Sensor Networks", International Journal of Science and Research, 2003.

[2] Government Health Staff, "Internet of Things triggers healthcare security concerns", Government Health IT, 2015

[3] Jun Shang, *et al.*, "Improvement of approach to detect sinkhole attacks in Wireless Sensor Networks", Intelligent Computing and Education Technology, pp 695

[4] Omprakash Gnawali, et al., "Collection Tree Protocol".

[5] Ioannis Krontiris, et al., "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks", 2007.

[6] Anthonis Papadimitriou, et al., "Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks", IEEE, 2009.

[7] Yong Wang, et al., "An Efficient Scheme for Removing Compromised Sensor Nodes from Wireless Sensor Networks", CSE Technical Reports, 2007.

[8] Qiang Wang, *et al.*, "Reprogramming Wireless Sensor Networks: Challenges and Approaches", IEEE, 2006.