CHAPTER 1

INTRODUCTION

In this chapter, Section 1.1 briefly introduces the two emerging applications of Wireless Ad hoc Networks (WANETs), namely Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). Section 1.2 introduces the MANET routing protocols. Section 1.3 introduces the concept of data aggregation in WSNs. Section 1.4 presents the vulnerabilities of WANETs. Section 1.5 presents the motivation of this thesis. The objectives and scope of this thesis are explained in Section 1.6. Finally, Section 1.7 outlines the organization of this thesis.

1.1 WIRELESS AD-HOC NETWORKS

WANETs are the distributed, dynamic, self-configuring, and decentralized wireless networks. Communication between nodes in these networks takes place with wireless links and without the help of a centralized trusted authority. This ad-hoc and decentralized working enabled them to be applied in the remote, hostile, and resource-constrained environments to perform mission critical tasks. Mostly, WANETs work with unlicensed ISM (Industrial, Scientific, and Medical) 868 MHz, 914 MHz, and 2.4 GHz wireless frequency bands [1, 2]. The following section introduces the two emerging applications of WANETs: MANETs and WSNs.

1.1.1 MOBILE AD-HOC NETWORKS

A MANET is an infrastructure-less and self-configurable mobile wireless network. In this, a collection of ubiquitous and mobile devices such as personal digital assistance, laptops, mobile phones, walkies-talkies, etc., communicate via limited bandwidth wireless channels [3].

1.1.1.1 MANET Characteristics

- **Autonomous operations**: Nodes communicate among them with inherent trust, cooperation, and without a central authority. Nodes act as the router to identify the path, and as the host to generate the data and control packets.

- **Dynamically changing topology**: Nodes arbitrarily move in the network with varying speed and direction. With this, nodes frequently enter and leave the communication range
of other nodes. It causes a dynamic change in topology.

- **Multi-hop routing:** Each node consists of a fixed communication range and hence they tend to follow multi-hop routing to transmit the data between the source and the destination nodes.

### 1.1.1.2 MANET Limitations

- **Node Heterogeneity:** A MANET often consists of nodes with dissimilar physical and functional characteristics. Due to different physical characteristics, nodes in the network consist of different communication ranges and it leads to asymmetric wireless links.

- **Resource Limitations:** Nodes in MANET consist of limited resources such as low processing power and a small memory size. Further, nodes consist of limited communication range and use limited bandwidth wireless channels.

### 1.1.1.3 MANET Applications

Due to the open and decentralized nature of operations, MANETs are used in the applications such as tactical networks – for military and battlefield surveillance; emergency services – for rescue and disaster recovery operations; data sharing – for multimedia data transmission; commercial and civilian environments – for vehicular services; context-aware services – call forwarding and mobile work-space; and coverage extension of cellular network access [4, 5].

### 1.1.2 WIRELESS SENSOR NETWORKS

WSNs are highly distributed wireless networks. In these networks, nodes are densely distributed to monitor and report the environment or physical conditions such as temperature, pressure, humidity, etc. Sensor Nodes (SNs) in the WSN consist of sensing and communication capabilities.
with small communication range, processing speed, memory size, and battery energy as compared to nodes in MANET. As shown in Figure 1.1, the hardware system of SNs consists of sensing subsystem, processing subsystem, communication subsystem, and power supply subsystem. Nodes sense the environment and process it using processing subsystem. Then, nodes forward the sensor data to the Base Stations (BS) directly or via multi-hop [2, 6].

1.1.2.1 WSN Characteristics

- **Power management:** WSNs, once deployed, tend to monitor the application for a long period. In this process, nodes spend most of the time in sleep mode to save battery energy. In sleep mode, nodes switch to low power mode by turning off their transceivers.

- **Dense deployment:** Nodes in WSN are densely deployed to monitor the environmental conditions. Dense deployment leads to overlap of communication ranges and hence BS may receive redundant data from the nodes.

- **Self-configuration:** SNs are often placed in resource-constrained environments and hence nodes need to be self-organized to form an ad-hoc route to the destination.

1.1.2.2 WSN Limitations

- **Frequent topology changes:** Topology of WSN often changes due to the wireless signal fading, low energy, and hardware failures.

- **Resource limitation:** WSNs are composed of SNs with small hardware configurations and energy resources. For example, MICAz [2] sensor node is assembled with an Atmel ATmega128L micro-controller with 128KB programmable flash memory, 4KB EEPROM, 512KB measurement flash memory, IEEE 802.14.5 compliant radio frequency transceiver, and energy supplied by two AA batteries.

- **Remote deployment:** WSNs are often deployed in remote and hostile environments such that nodes are prone to physical capture and reprogramming by anyone who access the deployment area.

- **Lack of tamper proof bodies:** Generally, SNs are not encapsulated by tamper proof bodies to save manufacturing cost. It gives scope for an intruder to physically capture and tamper the code from the node.

1.1.2.3 WSN Applications

WSNs have gained significant attention in the applications such as industrial monitoring, home automation, patient monitoring in health care, environment monitoring, machine-to-machine
communication, battlefield surveillance, fire in forest monitoring, disaster relief, emergency rescue operations, smart grids, smart cities, Internet of Things (IoT), etc. [4, 6, 7].

1.2 MANET ROUTING PROTOCOLS

Routing is the process of discovering routes between the source and the destination nodes. It is the fundamental functionality in any communication network. Conventional routing protocols designed for the wired network are insufficient for MANETs due to their characteristics such as dynamic topology, openness, and decentralized operations. Therefore, several efficient routing algorithms are proposed in the literature for effective data transmission in MANETs. These protocols are broadly classified into three categories: proactive, reactive, and geographic position-based routing protocols. Nodes running these protocols discover their neighbors by periodically broadcasting HELLO messages. HELLO messages are control packets, which consist of node information such as node identity (ID) and/or geographic position information. Nodes running routing protocols use this information to create neighbor table and to maintain the routing table for creating and updating routes. The rest of the section introduces the working principles of these protocols [3, 8, 5].

1.2.1 PROACTIVE ROUTING

Proactive routing is also said to be table-driven routing. As the name indicates, nodes running these protocols maintain the routes to all nodes in their routing table in advance. These protocols require different intermediate tables to update the path in the routing table. Since routes are readily available, these protocols transmit the data with a very low end-to-end delay. However, these protocols incur high routing overheads if the number of nodes in the network increases. It is because each node has to maintain the link state information of all nodes in the network. Further, these protocols result in high packet loss in high node mobility. Therefore, these protocols are not suitable for a large network with frequent topological changes. The OLSR (Optimized Link State Routing) protocol [9] and DSDV (Destination Sequence Distance Vector) protocol [10] are examples of this category.

1.2.2 REACTIVE ROUTING

In reactive routing, a source node establishes the path to the destination node when it has to transmit the data packets. In other words, the route between the source and the destination is established on demand. This dynamic route discovery sometimes leads to high end-to-end delay. Usually, these protocols initiate the route discovery by flooding the Route REQuest (RREQ) message in the network. The AODV (Ad-hoc On-demand Distance Vector) protocol [11], DSR (Dynamic Source Routing) protocol [12], and TORA (Temporally Ordering Routing Algorithm) [13] are examples of this category.
1.2.3 GEOGRAPHIC POSITION-BASED ROUTING

In this protocol, the routing takes place with node’s geographic position information [8, 14]. Nodes running this protocol need to know their geographic location. The location information may be obtained from Global Positioning System (GPS) attached to the node. Geographic routing results in very low end-to-end delay as compared to reactive routing protocols. The GPSR (Greedy Perimeter Stateless Routing) protocol [15] and GEAR (Geographic Energy Aware Routing) protocol [16] are examples of this category.

1.3 DATA AGGREGATION IN WSN

Data Aggregation (DA) is the process of gathering and summarizing the sensor data for statistical analysis [17]. The task of SNs in WSN is to sense the environment and broadcast the sensor data to the BS. Studies conducted by Wanger et al. [18] and Krishnamachari et al. [19] have shown that nodes spend more energy if they directly communicate sensor data to the BS. These studies have concluded that nodes could save 70% of their energy if they report the sensor data via multi-hop. As the SNs are densely deployed in the network to monitor the phenomena, data reported by SNs may result in redundant data due to overlapping communication ranges. Therefore, the DA process requires eliminating redundant data and energy efficient communication. To achieve this, Heinzelman et al. [20] proposed the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. It is a distributed and hierarchical clustering protocol for energy efficient DA in WSN. This concept has been enhanced by researchers further to optimize the network lifetime [21]. Clustering is the process of grouping the SNs in WSN. In the hierarchical clustering, the network is organized into a hierarchy of clusters with the BS at root as shown in Figure 1.2. Broadly, there exist three categories of nodes in the hierarchical clustering process: BS, Cluster Head (CH), and normal SN or non-CH nodes. BS periodically queries the network
for data collection. After receiving BS query, nodes initiate the setup and steady state phases. In the setup phase, cluster formation takes place and the data transfer takes place in the steady state phase.

1.3.1 SETUP PHASE

In this phase, a set of nodes elect themselves as CH. To do this, each node picks a random number \((R_n)\) between 0 and 1, and this value is compared with a threshold \(T(n)\) value calculated as follows [20]

\[
T(n) = \begin{cases} 
\frac{P}{1-P*(r \bmod \frac{1}{P})} & \text{if } n \in G \\
0 & \text{otherwise}
\end{cases}
\]  

In Eq.(1.1), \(P\) is the percentage of CHs, \(r\) is the query or round number, and \(G\) is the number of nodes that are not yet been CH in first \(1/P\) rounds. If a node’s \(R_n\) is less than \(T(n)\) then it becomes CH and broadcasts CH advertisement (CH_ADV) message. Upon receiving CH_ADV message, all the non-CH nodes decide on the cluster to which they want to belong based on shortest CH distance and residual energy. Then, to inform that they will be members of the cluster, non-CH nodes send CH join (CH_JOIN) message to CH node. In this way, setup phase ends with the CH election and cluster formation.

1.3.2 STEADY STATE PHASE

Upon receiving all the CH_JOIN messages from the non-CHs that would like to join the cluster, the CH node creates a TDMA (Time Division Multiple Access) schedule by assigning each node a time slot for the data transfer. CH broadcasts the schedule such that all the nodes in the cluster beware of their respective time slots. During the scheduled slots, the SNs transmit the sensor data to the CH. CH then aggregates the collected data using an aggregation operation such as SUM, MAX, MIN, AVG etc., and report aggregated data to any CH node or to the BS. After completing the data transmission, nodes in the network go into sleep mode. Nodes initiate the setup and steady state phase again when they receive a new query from BS.

1.4 VULNERABILITIES OF WANET

Due to the characteristics and limitations of WANETs such as the absence of infrastructure, distributed network operations, and dynamic topological changes, the network performance directly depends on the nodes cooperation in the network operations. Furthermore, communication protocols in WANETs are designed with an assumption that nodes are cooperative and trustworthy. In this context, node cooperation and its operational efficacy cannot be guaranteed in the presence of adverse activities. Figure 1.3 shows that how the lack of coordination among nodes affects various layer of node’s TCP/IP protocol stack. This lack of coordination
Figure 1.3: Security issues in TCP/IP protocol stack

<table>
<thead>
<tr>
<th>TCP/IP layer</th>
<th>Security issue(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>Worms, malicious codes, and viruses</td>
</tr>
<tr>
<td>Transport layer</td>
<td>End-to-end communication failure</td>
</tr>
<tr>
<td>Network layer</td>
<td>Disruption of routing paths</td>
</tr>
<tr>
<td>Data link layer</td>
<td>Link layer failures</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Signal jamming and denial-of-service</td>
</tr>
</tbody>
</table>

is said to be node misbehavior. The node misbehavior may occur in the following three ways [22, 23, 24, 25]

1. **Node malfunctioning:** Nodes in the network malfunction due to hardware or software problems. These are not malicious nodes. Buffer overflow and route error due to mobility are the examples of this category.

2. **Passive attack behavior:** Nodes in the network eavesdrop, impersonate, or creates a Denial of Service (DoS) on the communication between genuine nodes.

3. **Active attack behavior:** In this, although nodes appear to be legitimate and valid, they are being compromised by an adversary. These attacks are termed as internal security attacks. Internal attacks cannot be identified by conventional cryptography security methods. Systematic observation and assessment of node behavior help in isolating these attacks.

There exist two categories of active attacks: 1) Selfish behavior and 2) malicious behavior. Figure 1.4 shows the flow graphs of selfish and malicious behavior. Selfish behavior (or selfish attack) is an active attack and a selfish node does not cooperate in the network operations due to the resource limitations (such as low battery energy, to preserve bandwidth etc.). A shown in Figure 1.4a, a selfish node does not participate in the route establishment process and it does not cooperate in the packet forwarding. However, the selfish node communicates with the neighbors if it wants to send the data. On the other hand, as shown in Figure 1.4b, malicious behavior nodes do not obey the protocol operations. They thwart the routing process by launching various security attacks described as follows [26, 27, 28, 29, 30, 31, 32]:

1. **Flooding attack:** An attacker floods the control packets received from its neighbors to nodes in other parts of the network with the aim of increasing the congestion in the network

2. **Black-hole attack:** Malicious nodes simply drop the packets that they receive.
3. **Packet modification attack:** When a malicious node has to forward the packet, it changes the packet header information and forwards further. Such packets lose data integrity and due to which the packet-receiving node drops it as invalid.

4. **Gray-hole attack:** A malicious node selectively forwards the received packets. It also performs packet modification attacks. Gray-hole attack is also said to be selective forwarding attack.

5. **Energy based attack:** To beware of residual energy of nodes during routing, in some routing protocols nodes inform their residual energy periodically to their neighbors. In this context, a malicious node reports high residual energy than it actually consumes to drop the packets by attracting the traffic.

6. **Packet delay attack:** In DA, BS or CH has to receive the packets from the nodes within a time limit. However, malicious nodes delay the packet transmission and forward the packets after the time schedule. In this context, BS or CH does not consider such packets as fresh and hence discards from decision-making.

7. **Sybil attack:** The essential operations in WANETs such as routing and DA are carried out using node identity and/or location information. However, in Sybil attack, malicious
nodes deliberately report false identities and/or location information to disrupt the network operations.

8. **Badmouth attack:** A badmouth attacker provides false trust opinions to damage well-behaving node’s reputation by continuously advertising poor trust value.

9. **False data attack:** In WSNs, BS performs application dependent operations based on the sensor data received from the network. However, in this attack, malicious nodes deliberately report false sensor data to mislead the decision making process of BS.

10. **On-off attack:** A malicious node behaves good and bad alternatively to remain undetected while causing damage to the network.

11. **Wormhole attack:** Two or more malicious nodes collude to form a low latency link. This link appears as the shortest path in the routing. Benign nodes may choose this path to forward the packets. Once this path has been chosen, wormhole attackers in the path may drop or modify the packets.

### 1.5 MOTIVATION

Due to the openness and infrastructure-less network operations, MANETs and WSNs have gained significant attention in performing mission critical tasks in remote and hostile environments. Nevertheless, the limitations of these networks such as utilization of insecure wireless channels, remote deployment, distributed communication, self-organization, self-configuration, and utilization of limited bandwidth wireless channels introduce several security vulnerabilities. Further, nodes are subject to physical capture and tamper by an adversary due to lack of tamper proof bodies [33, 34]. An adversary may extract the information of nodes such as identity, location data, and secret key material. These tampered nodes may be kept back in the network to gain control over the network activities. These compromised nodes may exhibit malevolent behavior and thwart the network operations by launching various security attacks. The behavior of a compromised node can be either selfish or malicious [27, 28, 29]. Selfish behavior node does not harm the network operations; however, it does not cooperate in the network operations due to the resource limitations (such as low battery energy or to preserve bandwidth). On the other hand, malicious behavior is an active attack in which the compromised nodes intentionally harm the network operations.

Consider a MANET routing scenario shown in Figure 1.5. In this, each node has a fixed communication range and moves in the network with varying speed and direction. Let A be the source node and it has to forward the data to node H. Due to the limited communication range, A follows multi-hop communication and forwards the packet along the path (say A - B - E - F - H). Assume that node C is a malicious node and due to mobility node E has moved
away from the path and C has arrived in between nodes B and G. Since, C is the only available node to forward the data, B has to forward the packets to C. At this point, C may exhibit its malicious behavior by creating DoS [25, 26], dropping the data packets (black hole), selectively forwarding the packets (gray-hole), providing false identities and location information (Sybil attack), falsifying secondary trust values (badmouth attack), providing false residual energy (energy based attack), and exhibiting transient behavior (on-off attack) [29]. These attacks are said to be internal security attacks. These attacks show an adverse impact on the basic operations such as routing and data aggregation. Research studies have shown that the network performance metrics such as packet delivery ratio, throughput, energy consumption, and end-to-end delay will be greatly degraded in the presence of internal security attacks [29, 30, 31, 32]. It is because, in WANETs, the communication among nodes will take place by assuming nodes are trustworthy and cooperative in the network operations. Conventional routing and data aggregation protocols in these networks are designed based on this assumption. Due to this severity, identification and isolation of aforementioned attacks in these networks are an active research area.

Several hard security methods are proposed by the researchers to address the security attacks using conventional cryptography techniques [35, 36]. These methods utilize symmetric or asymmetric key cryptography that offers the security requirements such as confidentiality, integrity, authentication, non-repudiation, and access control. However, the essential steps of cryptographic methods such as key generation, key distribution, and re-keying result in high processing and communication overhead. In addition, cryptography security is inadequate in the presence of node misbehavior and internal attacks. It is because an adversary can start security attacks with the security keys obtained from compromised nodes. To this end, alternative methods are required to mitigate the security issues that arise due to internal security attacks.

Soft security is a type of security mechanism used in open systems to ensure security via social control [37]. A Trust Management System (TMS) is a soft security system, which is used to overcome the limitations of cryptography based security systems. A TMS is designed to avert harm or damage posed by the malicious nodes to the network. TMSs have received
considerable attention in various computer science allied fields such as electronic commerce and distributed computing. In WANETs, TMSs are used for improving cooperation among nodes in the presence of malicious activities while executing the application tasks such as routing and data aggregation. The objective of using these systems is to dynamically identify and isolate malicious nodes from protocol operations. Further, they calculate the trust value quantitatively based on the sincerity in executing the network protocols. This trust value is used to aid decision-making during routing and data aggregation with the goal of improving the network performance metrics in the presence of malicious activities. Therefore, the synergistic operation of cryptography methods and TMSs provides a complete security system.

1.6 OBJECTIVES AND SCOPE OF THIS THESIS

As mentioned in Section 1.5, node misbehavior is a vital factor that affects the network performance metrics. Therefore, this thesis considers the fundamental security problem in WANETs, “the protection of its basic functionality to route the data packets from the source to the destination with the mutual cooperation of nodes”.

Nodes misbehavior could be assessed by evaluating the trust value with the systematic observation of their social and functional behavior. To this end, “the objective of this thesis is to develop trust management based security methods for ensuring the cooperation among nodes and to improve the network performance in the presence of malicious nodes in MANETs and WSNs. These methods are used for dynamic detection and isolate the malicious nodes from the protocol operations such as routing and data aggregation”.

Security in communication networks is considered as a cross-layer issue. The security solutions designed for communication networks have to guard each layer of the protocol stack [27, 30]. The scope of this work is to identify and isolate malicious activities that affect the network layer functionality of the wireless networks protocol stack. As a part of it, a Generalized Trust Model (GTM) is proposed for improving cooperation among nodes. The proposed GTM is placed above the network layer of the node’s protocol stack as shown in Figure 1.6. GTM observes each trust metric defined to identify malicious nodes launching multiple security attacks in the network. Unlike existing trust model, GTM has the features such as systematic trust evidence collection, dynamic trust update, adaptive calculation of weight factors for trust metrics, an efficient method for filtering false recommended trust values, and a lightweight reputation exchange protocol. GTM is a distributed trust model that evaluates the Consolidated Trust Value (CTV) of nodes using direct and indirect observations.

The novelty of the proposed GTM is that it can adapt to any routing and DA protocol with little or no modifications. To show this, the GTM is integrated with the three MANET routing protocols: such as OLSR (proactive routing) protocol, AODV (reactive routing) protocol, and GPSR (geographic position-based routing) protocol. These protocols utilize the evaluated CTV to establish the trustworthy paths. Since CTV assessed by GTM is a Behavior based Trust (BT)
value, GTM with OLSR is termed as BT-OLSR, the integration of GTM with the AODV is termed as BT-AODV, and GTM with GPSR is termed as BT-GPSR. Further, GTM is customized to aid the location-aware routing in WSNs and it is termed as Trust and Location-Aware Routing (TLAR) protocol.

Further, a Trust-aware Data Aggregation and Intrusion Detection System (TDAGIDS) is proposed to show that the proposed GTM is also suited for improving cooperation among nodes during DA process. With the evaluated CTV of nodes, an Intrusion Detection System (IDS) is placed at the BS to analyze and identify the malicious nodes by running a statistical test.

Node identity and location information are the two vital factors that help routing and data aggregation in ad-hoc and sensor networks. However, the performance of these protocols will affect severely if malicious nodes deliberately report false identity and/or location information. This malicious behavior is said to be the Sybil attack. Therefore, the final part of the work presents the proposed Sybil Attack Detection using Sequential Analysis (SADSA) method for static WSNs. SADSA method has two stages: 1) evidence collection and 2) evidence validation. In the first stage, the evidences that are required to prove a node as malicious are collected and consolidated. In the second stage, consolidated evidences are validated using Sequential Probability Ratio Test (SPRT) for improving the Sybil attack detection accuracy. The novelty of this method is that it is purely node centric and does not have additional overheads.

Figure 1.7 depicts the schematic diagram of the research work reported in this thesis. The performance of the proposed soft security methods is evaluated using the ns-2 simulator under various simulation scenarios. After literature survey in Chapter 2, Chapter 3 to Chapter 6 presents the proposed methods and their performance evaluation.
1.7 ORGANIZATION OF THIS THESIS

Figure 1.8 shows the block diagram of the organization of this thesis. This thesis consists of seven chapters. Description of these chapters is as follows

Chapter 1 is this chapter. It introduces WANET categories, WANET routing protocols, data aggregation in WSNs, and security vulnerabilities of WANET. Further, this chapter also provides the objectives and scopes of this research work.

Chapter 2 discusses the related work on trust management models in wireless ad-hoc and sensor networks. It describes the state-of-the-art trust management based security methods to deal with security vulnerabilities with their advantages and limitations.

Chapter 3 presents the proposed Generalized Trust Model. First, it introduces motivation behind proposing the GTM and then describes the working procedure in detail. Next, integration of GTM into MANET routing protocols: OLSR, AODV and GPSR protocols are explained. It
describes how CTV is used for establishing trustworthy paths in the routing table. Finally, this chapter shows how GTM is customized for location-aware routing in WSNs.

**Chapter 4** presents the performance evaluation of GTM with MANET and WSN routing protocols with existing trust models in various simulation scenarios using the network simulator ns-2. The performance evaluation considers the network performance metrics such as packet delivery ratio, end-to-end delay, routing load, and energy consumption. Further, direct trust module of the GTM is implemented using nesC programming in TinyOS environment and validated in a WSN testbed consists of 15 TelosB SNs.

**Chapter 5** is an extension of Chapter 3. In this Chapter, the proposed GTM is modified for collaborative TDAGIDS in WSN. It is shown that the proposed GTM is also suited for improving cooperation among nodes during DA process. The modified GTM is termed as M-GTM. This M-GTM is placed at the node level and an IDS is placed at the BS level. Nodes calculate CTVs of their neighbors and report these values to the BS along with the sensor data. Then, IDS at BS analyzes the CTVs received from the network nodes and prepares a malicious list by running a statistical test. This malicious list is informed to nodes along with the next query. In this way, M-GTM at the node level and IDS at the BS level collaboratively identify and isolate malicious nodes from DA process. Finally, the performance of TDAGIDS is evaluated against the existing trust based DA methods using the ns-2 simulator.

**Chapter 6** first introduces the motivation behind proposing SADSA method. Next, it describes the design and implementation of the proposed SADSA method in detail. SADSA method is designed to detect malicious nodes that perform Sybil attack by sending out 1) a false identity and correct location information, 2) correct identity and false location information, and 3) both false identity and location information. Furthermore, SADSA method is integrated with GPSR protocol to identify Location Based Attacks (LBAs). The significance of this work is to show that the SADSA method can work hand-in-hand with underlying protocols. Finally, the performance of SADSA method is compared with existing Sybil attack detection methods using the ns-2 simulator.

**Chapter 7** concludes the thesis with the recommendations for future work.