# Mrakov Chain Monte Carlo Based Internal Attack Evaluation for Wireless Sensor Network

**Muhammad R Ahmed†, Xu Huang† and Hongyan Cui††**

†Faculty of Information Sciences and Engineering, University of Canberra, Australia

††School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, China

**Summary**

Wireless Sensor Networks (WSNs) consists of low-cost and multifunctional resources constrain nodes that communicate at short distances through wireless links. It is open media and underpinned by an application driven technology for information gathering and processing. It can be used for many different applications range from military implementation in the battlefield, environmental monitoring, health sector as well as emergency response of surveillance. With its nature and application scenario, security of WSN had drawn a great attention. It is known to be valuable to variety of attacks for the construction of nodes and distributed network infrastructure. In order to ensure its functionality especially in malicious environments, security mechanisms are essential. Malicious or internal attacker has gained prominence and poses the most challenging attacks to WSN. Many works have been done to secure WSN from internal attacks but most of it relay on either training data set or predefined threshold. Without a fixed security infrastructure a WSN needs to find the internal attacks is a challenge. Normally, internal attack's node behavioural pattern is different from the other neighbours, called "good nodes," in a system even neighbour nodes can be attacked. In this paper, we have proposed a new approach for detecting internal attack by using Mrakov Chain Monte Carlo (MCMC). It is an efficient real time algorithm. It is good for sensor network as it operates with no or incomplete classification information. Our result shows the output of the internal attacker evaluation.

***Key words:***

*Wireless Sensor Network (WSN), internal attack, Markov Chain Monte Carlo, Security.*

## 1. Introduction

A Wireless Sensor Network (WSN) consists of a large number of low-cost, low-power, multifunctional and resource-constrained sensor nodes with each sensor node consisting of sensing, data processing, and communicating components; these nodes can operate unattended for long durations. Sensor networks are designed with the flexibility to withstand harsh environmental conditions. These are networks of wireless interconnected smart devices designed and deployed to retrieve sensor data of interest from their host environments. Sensor nodes perform measurements of some physical phenomena, collect and process data, communicate with other peers or a central information processing unit, the sink. These nodes are capable of sensing various phenomena, such as Pressure, Temperature, Humidity, Position, Velocity, Acceleration, Force, Vibration, Proximity, Motion, Biochemical agents, etc.[1][2][3][4][5][6][7] They are capable of processing textual, voice and video data making them very useful. According to the applications the deployment strategy is decided [8]. When the environment is unknown or hostile such as remote harsh fields, disaster are as toxic environment the deployment usually done by scatter by a possible way, sometimes by small an aircraft. Thus the position of the sensor nodes may not be known in advance. In the post deployment the sensor nodes perform self-organization mechanism to set up the network by determining the neighbor and setting up the routing table by themselves in an autonomous way. A typical WSN shown in Figure 1.

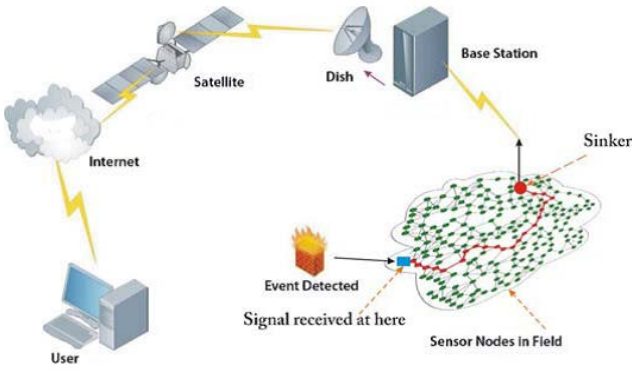


Figure 1. A typical WSN

In all communication networks including WSN, security provisioning is a critical requirement. Security in the wireless sensor network is challenging and important task because of its characteristics that includes open nature of wireless medium, unattended operation, limited energy, memory, computing power, communication bandwidth, and communication range. Hence, it is more susceptible to the security attack in comparing to the traditional wired network. The security of WSN can be investigated in in different perspectives, for example WSN attacks can be classified as two major categories: *external* and *internal*

Manuscript received March 5, 2013
Manuscript revised March 20, 2013

attacks according to the domain of attacks [8]. External attack is defined as the attack does not belong to the network and it does not have any internal information about the network such as cryptographic information. When a legitimate node of the network acts abnormally or illicit way it is consider as a suspect of an internal attack. It uses the compromised node to attack the network which can destroy or disrupt the network easily. In this paper we focus on the internal attacks.

Considering the characteristics of WSN many algorithms have developed for the secure functionality of WSN. Most of the work has focused on the pair wise key establishment, authentication access control and defence against an attack. Most importantly those works mainly focused on the traditional cryptographic information, data authentication in order to build the relationships among the sensors. But, the cryptographic methods sometimes are not very efficient and effective. The unreliable communications through wireless channel can make the communication technique vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary [9]. The compromised entity of the network appears as a legitimate node. So it is easy for the adversary to launch the internal attacks. When internal attack occurs for a node, this node will behave abnormally such as tampering the massage from other member, dropping the data or broadcast excessive data.

Although WSN shares many properties with Wireless ad hoc network and may require similar techniques such as routing protocols but in certain cases it directly prohibit using the protocols proposed in wireless ad hoc network. Thus, the characteristics and architecture differs as well. To demonstrate this issue, the dissimilarities between the WSN and wireless ad hoc network are summarized: [10]

- The number of sensor nodes (hundreds or thousands nodes) in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed, so multiple sensors can perform to measure the same or similar physical phenomenon.
- Sensor nodes are prone to failures because of battery exhaustion and hostile environment.
- The topology of a sensor network changes very frequently caused by node failure.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

The unique properties and characteristics of WSN need to be considered in order to secure the WSN. Many algorithms have developed for the secure functionality of WSN. Most of the work has focused on the pair wise key establishment, authentication access control and defense against attack. Most importantly those works mainly focused on the traditional cryptographic information, data authentication in order to build the relationship between the sensors. However, the unreliable communications through wireless channel made the communication technique vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary [11]. The compromised entity of the network acts as a legitimate node. So it is easy for the adversary to perform the internal attacks. When internal attack occurs for a node, this node will behave abnormally such as tampering the massage from other member, dropping the data or broadcast excessive data.

So far, not much attention has been given to protect the network from the internal attack. In this paper, we have used MCMC- MH algorithm to detect the internal attack of WSN. With the MCMC method, it is possible to generate samples from an arbitrary posterior density and to use these samples to approximate expectations of quantities of interest. [12]Moreover, it works in real time by constricting the sample chain and compute the changes and come up with a acceptance ratio. We decide the internal attacker based on the acceptance ratio..

The paper is organized as follows: section 2 is comprised of the applications of WSN overview of Main type of Internal Attacks discussed in section 3 followed by the related work in section 4. Section 5 is network assumption and method. This section covers the details of internal attacker identification process. The efficiency of the framework is presented in Result section in section 6 followed by conclusion in section 7.

## 2. Applications of WSN

WSNs can be used in large number of different applications based on the category of the sensors. Even though WSN was originated for military application but recently it’s implemented in several civil sector as well. They are used in commercial and industrial applications to monitor data that would be difficult or expensive to monitor using wired sensors. They could be deployed in wilderness areas, where they would remain for many years (monitoring some environmental variable) without the need to recharge/replace their power supplies. They could form a perimeter about a property and monitor the progression of intruders (passing information from one node to the next).

Typical applications of WSNs include monitoring, tracking, and controlling. Some of the specific applications are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring, etc. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. WSNs have been investigated. e.g, [13]

- Environmental monitoring
- Habitat monitoring
- Acoustic detection
- Seismic Detection
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

## 3. Main Types of Internal Attacks in WSN

Simple sensor nodes are usually not well physically protected due to they are cheap and are always deployed in open or even in hostile environments where they can be easily captured and compromised, hence, an adversary can extract sensitive information, control the compromised nodes and let those nodes service for the attackers. The attacks are involved in corrupting network data or even disconnecting major part of the network. The compromised node holds the following characteristics [14]:

- It usually runs some malicious code that is different from the code running on a legitimate node and seeks to steal information from the sensor network or disrupt its normal function.
- Node uses the same radio frequency as the other normal sensor nodes so that it can communicate with them.
- Node is authenticated and participates in the sensor network. Since secure communication in sensor networks is encrypted and authenticated using cryptographic keys, compromised nodes with the secret keys of a legitimate node can participate in the secret and authenticated communication of the network.

It is obviously that the compromised nodes are more dangerous as the adversary can easily obtain the access information from the cryptographic information and then to make further attacks with the trust of other sensors. This type of attack is difficult to break or stop. That is why it has become a challenging task to secure WSN from internal attack.

In many applications, the data obtained by the sensing nodes needs to be kept confidential and it has to be authentic. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network. The major attacks are: Denial of Service (DOS), Worm hole attack, Sinkhole attack, Sybil attack, Selective Forwarding attack, Spoofed and Altered, or Replayed routing information, Hello flood attack, flooding attack. Based on the Opes System Interconnect (OSI) model the attack can be tabulated in table 1 [15]:

Table 1: Layer Based Security Attacks [16]

| Layer | Attacks |
|---|---|
| Physical layer | Jamming, Tampering, Sybil Attack |
| Data Link Layer | Collision, Sybil Attack, Spoofing and Altering Routing Attack, Replay attack |
| Network Layer | Internet smart attack, Sybil Attack, Blackhole Attack, Spoofing and Altering Routing Attack, wormhole attack, selective forwarding attack, Hello Flood Attack. |
| Transport Layer | Flooding Attack, Desynchronisation |
| Application | Spoofing and Altering Routing Attack, False Data Injection, |

1. *Denial of Service (DoS) attacks*

Denial of service attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: Jamming, Tapering, collision, Homing, flooding, etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming. In WSN several types of Dos Can be performed in different layers which tabulated in the table 2 [15]

Table 2: Layer Based DoS attack [17]

| Layer | Attacks |
|---|---|
| Physical layer | Jamming, Tampering |
| Data Link Layer | Collision, Exhaustion |
| Network Layer | Misdirection |
| Transport Layer | Desynchronisation |
| Application Layer | Path Based DoS |

The discussed attacks are linking some terminologies that are defined as follows [16][17]:

Jamming: Jamming is a popular Denial of Service (DOS) attack. In this attack the attacker attempts to jam the frequencies of the radio used for communication between the nodes in the network. In this attack, an adversary may use e few nodes in strategic positions to effectively jam most of the communications inside the network. In essence, an attacker needs only a few nodes in order to disseminate a large network.

Tampering: Because of the nature of wireless sensor networks, an adversary could easily get physical access to the sensor nodes. This may enable an attacker to compromise sensor nodes in a DOS like manner

Collision: This is a DOS attack, where a node induces a collision in some small part of a transmitted packet. The packet will then fail the checksum check, because of the changes brought on by the collision, and the receiver node will then ask for a retransmission of the packet.

Exhaustion: This attack is a collision attack taken a bit further. A malicious node may conduct a collision attack repeatedly in order to exhaust the power supply of the communicating nodes.

Misdirection: In this attack a malicious node, that is part of a route, can instead of dropping packets, quite simply send them on a different path where there does not exist a route to the destination. The malicious node can do this for certain packets, or all packets.

Desynchronisation: it can disrupt an existing connection between two end points. Adversary transmits forget packet with bogus sequence number or control flag to degrade or prevent the exchange of data.

Path based DoS: An adversary overwhelms sensor nodes by flooding a multihope end to end communication path with either replayed or injected false message to injected false message to waste secure energy resources.

*2. Wormhole attack*

Just like the theoretical wormholes in space, this attacker can send packets, routing information, ACK etc, through a link outside the network to another node somewhere else in the same network. This way an attacker can fool nodes into thinking they are neighbours, when they are actually in different parts of the network. This can also confuse routing mechanisms that rely on knowing distances between nodes. A wormhole attack can be used as a base for eaves dropping, not forwarding packets in a DOS like manner, alter information in packets before forwarding them etc.

*3. Sinkhole attack*

This is a DOS attack, where a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a “low cost route first “protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths. The neighbours of this node will also chose this node in routes, and compete for the bandwidth. This way the malicious node creates a black hole inside the network.

*4. Sybil attack*

The Sybil attack targets fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. This is done by having a malicious node present multiple identities to the network. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once

*5. Selective forwarding attack*

In this attack, malicious nodes can decide not to forward packets of certain types or to from certain nodes. Even though the protocol is completely resistant to the sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch this type of attack if it is strategically located near the source or a base station.

*6. Spoofing attack*

In this attack, a malicious node may be able to create routing loops, wormholes, black holes, partition the network and etc., by spoofing, altering or replaying routing information.

*7. Hello flood attack*

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbours. A node receiving such a packet may assume that it is within the radio range of the sender but this assumption may be false.

*8. Flooding attack*

In this attack, a malicious node may send continuous connection requests to a victim node effectively flooding the victim’s network link

Unlike traditional routing, where intermediate nodes just forward input packets, in network coding intermediate nodes actively mix or code input packets and forward the resulting coded packets. The very nature of packet mixing also subjects network coding systems to a severe security threat, knows as a pollution attack, where attackers inject corrupted packets into the network. Since intermediate nodes forward packets coded from their received packets, as long as least one of the input packets is corrupted, all output packets forwarded by the node will be corrupted. This will further affect other nodes and result in the epidemic propagation of the attack in the network. In [15], it addressed pollution attacks against network coding systems in wireless mesh networks.

## 4. Related work

Traditionally Internal attack detection by misbehavior has produced in the literature for peer to peer and ad hoc networks, but for WSN little work has been done. With the indication of misbehavior of the node we can find the internal attack in the network. So far, security using internal attack detection based on abnormal behavior or misbehavior not given much attention. Abnormal behavior (misbehavior) of the node has been proposed in different research but main focus was given on preventing and securing routing from attacks.

Intrusion detection in Wireless sensor network is studied in [18][19], In [18] Zhang *et al.* proposed a scheme which is the first work on intrusion detection in wireless ad hoc networks. A new architecture is investigated for collaborative statistical anomaly detection which provides protection from attack on ad hoc routing. Silva *et al.* in [19] shows that an intrusion alarm is raised when number of failures exceeds a pre-defined threshold. This method the decision is made based on a simple summation of the rule whereas multiple rules have been defined.

To detect abnormal behavior Staddon *et al* [20] proposed to trace the failed nodes in sensor networks at the base station assuming that all the sensor measurement will be directed along the sinker based on the routing tree. In this work the sinker has the global view of the network topology and can identify the failed nodes through route update message and it is directional.

Watchdog like technique is proposed in [21][22] and [23]. The purpose of the watchdog mechanism is to identify a malicious node by overhearing the communication of the next hop. This technique can detect the packet dropping attack by letting nodes listen to the next hope nodes broadcasting transmission. Normally, multiple watchdog work collaboratively in decision making and reputation system is necessary to provide the quality rating of the participants.

Karlof and Wagner discussed attacks at the network layer in [24] and mentioned altered or replayed routing information and selective forwarding, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding. Some papers discussed various attacks in term of network's resiliency, such as [25], they discussed how to keep WSN routing protocols as stateless as possible to avoid the proliferation of specific attacks and provide for a degree of random behaviour to prevent the adversary from determining which the best nodes to compromise are. They defined three items, namely (i) average delivery ratio, (ii) average degree of nodes, and (iii) average path length to describe the networks resiliency. Obviously, the more efficient and effective ways are needed.

Unlike traditional routing, where intermediate nodes just forward input packets, in network coding intermediate nodes actively mix or code input packets and forward the resulting coded packets. The very nature of packet mixing also subjects network coding systems to a severe security threat, knows as a pollution attack, where attackers inject corrupted packets into the network. Since intermediate nodes forward packets coded from their received packets, as long as least one of the input packets is corrupted, all output packets forwarded by the node will be corrupted. This will further affect other nodes and result in the epidemic propagation of the attack in the network. [26] addressed pollution attacks against network coding systems in wireless mesh networks. They proposed a lightweight scheme, DART that uses time-based authentication in combination with random liner transformations to defend against pollution attacks.

A few papers also address pollution attacks in internal flow coding systems use special crafted digital signatures [27][28] or hash functions [29][30]. Recently some papers discuss the preventing the internal attacks by related protocols[31][32].

Recently Game theory is commonly used to analyze wireless networks with selfish/attacker nodes. Reddy and Ma studied game theory based approach in [33][34], Reddy *et al.* approach in [33] using zero-sum game may find malicious sensor nodes in the forwarding path only. This method need to maintain a certain level of energy. The proposed method in [34]not only improves the security of WSNs, but also reduces the cost caused by monitoring sensor nodes and prolongs the lifecycle of each sensor node. However, the method does not consider the effects of the selfishness of the sensor nodes, which can discard normal packets or not transfer normal packets in WSNs.

Most of the existing related works are for ad hoc networks. With the differences in WSN and Wireless ad Hoc network the security mechanism for ad hoc network cannot protect WSN completely. Moreover, it is well know that most of existing mechanisms are based essentially on cryptographic primitives. In cryptographic approaches, the source uses cryptographic techniques to create and send additional verification information that allows nodes to verify the validity of coded packets. Polluted packets can then be filtered out by intermediate nodes. The proposed schemes rely on techniques such as homomorphic hash functions or homomorphic digital signatures. These schemes have high computational overhead, as each verification requires a large number of modular exponentiations. In addition, they require the verification information, such as hashes or signatures to be transmitted separately and reliably to all nodes in advance, which is normally difficult to achieve efficiently in wireless networks.

## 5. Network assumptions and Method

The system under consideration consists of an area of interest where region wise detection requirements are provided by the end user. We model the area of interest as a grid Ω of $N_x \times N_y$ points. The ratio of the detection to miss requirements at every point on the grid are ordered in two $N_xN_y \times 1$ vector of the ratio of the probability, $p_d / p_m$. There are two common sensing models found in literature, binary detection model and the exponential detection model. Both models share the assumption that the detection capability of a sensor depends on the distance between the sensor and the phenomena, or target to be detected. Following [25] notations we have the case that for the binary detection model, the probability of detection $p_d\ (t, s)$ is given as:

$$p_d(t,s) = \begin{cases} 1 & \text{if } d(t,s) \le r_d \\ 0 & \text{if } d(t,s) > r_d \end{cases} \tag{1}$$

where $r_d$ is the detection radius and $d(t, s)$ is the distance between the target's position "$t$" and the sensor location "$s$" on a plane. The exponential model is a more realistic model, where the probability of detection corresponds to

$$p_d(t,s) = \begin{cases} e^{-\alpha d(t,s)} & \text{if } d(t,s) \le r_d \\ 0 & \text{if } d(t,s) > r_d \end{cases} \tag{2}$$

where ∝ is a decay parameter that is related to the quality of a sensor or the surrounding environment. In the exponential model of equation (2), even if a target is within the detection radius, there is a probability that it will not be detected, which means it will be missed. As this model is closer to the realistic case, we shall use this model.

The process of linking individual sensors' detection characteristic to the overall probability of detection requirements on the grid is mathematically quantified using miss probabilities, $p_{\mathrm{miss}} = 1 - p_{\mathrm{d}}$, where $p_{\mathrm{d}}$ is the probability of detection. The overall miss probability $M(x, y)$ corresponds to the probability that a target at point $(x, y)$ will be missed by all sensors, which is

$$M(x,y) = \prod_{(i,j)\in\Omega} p_{miss}((x,y),(i,j))^{u(i,j)} \tag{3}$$

where $u(i, j)$ represents the presence or absence of a sensor at the location $(i, j)$ on the grid, and corresponds to

$$u(i,j) = \begin{cases} 1, & \text{if there is a sensor at } (i,j) \\ 0, & \text{if there is no sensor at } (i,j) \end{cases} \tag{4}$$

Taking the natural logarithm of the both sides in equation (3), we have

$$m(x,y) = \sum_{(i,j)\in\Omega} u(i,j) \ln p_{miss}((x,y),(i,j)) \tag{5}$$

where $m(x, y)$ is so-called the overall logarithmic miss probability at the point $(x, y)$. Thus we have the function $b(x, y)$ as

$$b(x,y) = \begin{cases} \ln p_{miss}((x,y),(0,0), & d((x,y),(0,0) \le r_d \\ 0, & d((x,y),(0,0)) > r_d \end{cases} \tag{6}$$

The overall logarithmic miss probabilities for all points on the grid can be arranged in a vector m of dimension $N_{\mathrm{x}}N_{\mathrm{y}} \times 1$ that corresponds to equation (7) as shown below:

$$\mathbf{m} = [m(x,y), \forall (x,y) \in \Omega]^T$$
$$\mathbf{u} = [u(i,j), \forall (i,j) \in \Omega]^T$$
$$\text{and} \quad \mathbf{m} = \mathbf{Bu} \tag{7}$$

The $((i\ \text{-}1)N_{\mathrm{y}} + j)$-th element of u indicates the number of sensors deployed at point $(i, j)$ on the grid. The matrix **B** is of dimension $N_{\mathrm{x}}N_{\mathrm{y}} \times N_{\mathrm{x}}N_{\mathrm{y}}$, and it contains

$$\{b(x-i, y-j), \forall (x,y) \in \Omega, (i,j) \in \Omega\}$$

$b(x - i, y - j)$ corresponds to the $(r, c)$-th entry of **B**, where $r = (x -1)N_{\mathrm{y}} + y$ and $c = (i -1)N_{\mathrm{y}} + j$.

Essentially, $b(x - i, y - j)$ quantifies the effect of placing a sensor at the point $(i, j)$ on the logarithmic miss probability at the point $(x, y)$ on the grid. If there are some compromised nodes distributed in a WSN, how those compromised nodes could be detected by their so-called abnormal attributes among the network, such as irregular change of hop count that implicates sinkhole attacks; the signal power is impractically increasing which may indicate wormhole attacks; abnormally dropping rate traffic behaviours related the related nodes most likely to be compromised, etc. to find the compromised node we use Markov Chain Monte Carlo.

The Markov Chain Monte Carlo (MCMC) method approximates the recursive Bayesian filtering distribution as a set of discrete samples known as a Markov Chain. In order to do this, we follow the Monte Carlo approximation, where the prior is approximated by a set of samples.[35] In order to understand MCMC we have to understand Markov Chain (MC) and Monte Carlo(MC).

A Markov chain is a stochastic process where transition from one state to another state using a simple sequential procedure. We start a Markov chain at some state $x^{(1)}$, and use a transition function $p(x^{(t)}|x^{(t-1)})$, to determine the next state, $x^{(2)}$conditional on the last state. We then keep iterating to create a sequence of states Each such a sequence of states is called a Markov chain or simply chain:

$$x^{(1)} \to x^{(2)} \to \cdots \ldots . x^{(t)} \to \cdots \ldots \tag{8}$$

Monte Carlo integration is used to samples to approximate the expectation of a complex distribution. Specifically, we obtain a set of samples $x^{(t)}$ , $t = 1,2, \ldots \ldots N$ , drawn independently from distribution $p(x)$. If $g(x)$ is the function of expectation for the continuous random variable $x$. The expectation is defined as:

$$E[g(x)] = \int g(x)p(x)dx \tag{9}$$

The goal of MCMC is to design a Markov chain such that the stationary distribution of the chain is exactly the distribution that we are interesting in sampling from. This is called the target distribution. In other words, we would like the states sampled from some Markov chain to also be samples drawn from the target distribution. The idea is to use some clever methods for setting up the transition function such that no matter how we initialize each chain, we will convergence to the target distribution.

MCMC adopts the Metropolis-Hasting (MH) to generate the sample from the stationary distribution $p(x)$. The sequence of $x$ values denoted in such a way $(x_1, x_2, x_3 \ldots \ldots . . x_n)$ that $n \to \infty$. The target or candidate is denoted as $x^*$ so the proposal distribution becomes $Q(x^*|x_n)$ which depends on the current state of the Markov chain, $x_n$. Based on that we will decided that the target node transition is acceptable or not at a given time interval. [36] We will consider the node is internal attacker if the transition is not acceptable. The acceptance probability can be defined as.

$$A(x_n \to x^*) = min\left(1, \frac{p(x^*)Q(x_n|x^*)}{p(x_n)Q(x^*|x_n)}\right) \tag{10}$$

We have the proposed target or candidate $x^*$ and calculated acceptance probability $A(x_n \to x^*)$. now either decide to “accept” the candidate or target (in which $x_{n+1} = x^*$ or we decide to “reject” the target (in which $x_{n+1} = x_n$). Then we sample $u \sim U_{0,1}$.

$$x_{n+1} = \begin{cases} x^* & if \quad u \le A(x_n \to x^*) \\ x_n & if \quad u > A(x_n \to x^*) \end{cases} \tag{11}$$

In order to find the internal attacker in our case we can execute framework in the algorithm shown below.

```
Algorithm 1
I.     Set $x^0 = x_0$;
II.    Iteration $n, n \ge 1$;
  1. Sample a target or candidate $x \sim Q_1(x^* | x_n)$
  2. Evaluate the acceptance probability
     $A(x_n \to x^*) = \min\left(1, \frac{p(x^*)Q(x_n | x^*)}{p(x_n)Q(x^* | x_n)}\right)$
  3. Sample $u \sim U_{0,1}$.
III.   Go to II.

end
```

## 6. Result

Our temperature measurement wireless sensor network is simulated in MATLAB to find the internal attack. In the simulation we have implemented the Markov Chain Monte Carlo (MCMC) Metropolis-Hasting (MH) algorithm to see the node acceptance ratio with imperial data. In the simulation environment the parameter we set is as follows,,

Table 1: Parameter

| Parameters | Values |
|---|---|
| Packet Size | 500 bytes |
| Initial Energy | 2 J |
| Cluster Radius | 50m |
| Regional Area | (0,0) to (500,500) |

We ran the simulation for 50 samples with the sigma value 0.5. From the proposal distribution of the WSN we found the acceptance ratio of the suspected node or candidate is 28%. Which means the candidate is an internal attacker.

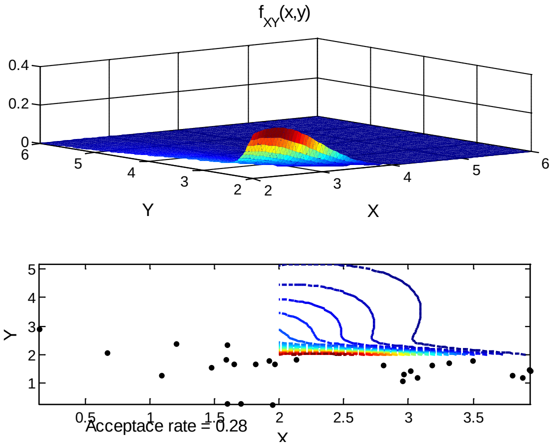


Figure 3. MCMC based node Acceptance Ratio

## 7. Conclusion

In this paper, we described about the main internal attacks in wireless sensor networks based on OSI layer and we have carefully investigated internal attacks for WSN and create a novel algorithm for protecting WSNs from the internal attacks based on Markov Chain Monte Carlo - Metropolis-Hasting. The simulation results, shows the acceptance rate of the candidate or internal attack.

In future, we would like to create a real time database for the nodes normal behaviour and simulate in the hardware platform.

### Acknowledgments

This project is supported by the Commonwealth of Australia under the Australia-China Science and Research Fund (ACSRF02541). One of authors would like to thank the work has been partly supported by the national Natural Science Foundation of China (Grant No. 61201153) the National 973 Program of China under Grant (No. 2012CB315805).

### References

[1] X. Huang, M. Ahmed, and D. Sharma, “Timing control for protecting from internal attacks in wireless sensor networks,” in *2012 International Conference on Information Networking (ICOIN)*, 2012, pp. 7 –12.

[2] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets,” *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 17 –29, Mar. 2002.

[3] C. Meesookho, S. Narayanan, and C. S. Raghavendra, “Collaborative classification applications in sensor networks,” in *Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2002*, 2002, pp. 370 – 374.

[4] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh, “Energy-efficient surveillance system using wireless sensor networks,” in *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, New York, NY, USA, 2004, pp. 270–283.

[5] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, “Distributed control applications within sensor networks,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1235 – 1246, Aug. 2003.

[6] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop-Hurley, “Wireless ad hoc sensor and actuator networks on the farm,” in *The Fifth International Conference on Information Processing in Sensor Networks, 2006. IPSN 2006*, 2006, pp. 492 –499.

[7] F. Zhao, “Wireless sensor networks: a new computing platform for tomorrow’s Internet,” in *Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging*

*Technologies: Frontiers of Mobile and Wireless Communication, 2004,* 2004, vol. 1, pp. I – 27 Vol.1.

[8] M. Ahmed, X. Huang, and D. Sharma, “A Taxonomy of Internal Attacks in Wireless Sensor Network,” in *World Academy of Science, Engineering and Technology*, Kuala Lumpur, Malaysia, 2012, pp. 427–430.

[9] M. Ahmed, X. Huang, D. Sharma, and L. Shutao, “Wireless sensor network internal attacker identification with multiple evidence by dempster-shafer theory,” in *Proceedings of the 12th international conference on Algorithms and Architectures for Parallel Processing - Volume Part II*, Berlin, Heidelberg, 2012, pp. 255–263.

[10] M. Ahmed, X. Huang, D. Sharma, and H. Cui, “Wireless Sensor Network: Cherecterestics and Architectures,” in *World Academy of Science, Engineering and Technology*, Penang, Malaysia, 2012, vol. 72, pp. 660–663.

[11] M. Ahmed, X. Huang, and H. Cui, “Smart Decision Making for Internal Attacks in Wireless Sensor Network|,” *International Journal of Computer Science and Network Security,*, vol. 12, no. 12, pp. 15–23, Dec. 2012.

[12] S. P. Brooks and G. O. Roberts, “On Quantile Estimation and Markov Chain Monte Carlo Convergence,” *Biometrika*, vol. 86, no. 3, pp. 710–717, Sep. 1999.

[13] T. Arampatzis, J. Lygeros, and S. Manesis, “A Survey of Applications of Wireless Sensors and Wireless Sensor Networks,” in *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005*, June, pp. 719–724.

[14] M.-Y. Hsieh and Y.-M. Huang, “Adaptive Security Modules in Incrementally Deployed Sensor Networks,” *International Journal on Smart Sensing and Intelligent Systems*, vol. 1, no. 1, pp. 70–86, Mar. 2008.

[15] K. Sharma and M. K. Ghose, “Wireless Sensor Networks: An Overview on its Security Threats,” *IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs; CSE Department*, vol. 1, no. 1, pp. 42–45, 2010.

[16] H. K. D. Sarma and A. Kar, “Security Threats in Wireless Sensor Networks,” in *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, Oct., pp. 243–251.

[17] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, “Attacks in Wireless Sensor Network,” vol. 5, no. 7, pp. 954–960, 2011.

[18] Y. Zhang and W. Lee, “Intrusion Detection in Wireless AdHoc Networks,” presented at the ACM MOBICOM, The Annual International Conference on Mobile Computing and Networking, Boston, Massachusesttes, USA, 2000, pp. 275–283.

[19] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, “Decentralized Intrusion Detection in Wireless Sensor Networks,” in *Proceedings Of The 1st Acm International Workshop On Quality Of Service & Security In Wireless And Mobile Networks (Q2SWINET’05)*, 2005, pp. 16–23.

[20] J. Staddon, D. Balfanz, and G. Durfee, “Efficient tracing of failed nodes in sensor networks,” in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, New York, NY, USA, 2002, pp. 122–130.

[21] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of the 6th annual international conference on Mobile computing and networking*, New York, NY, USA, 2000, pp. 255–265.

[22] K. Paul and D. Westhoff, “Context aware detection of selfish nodes in DSR based ad-hoc networks,” in *IEEE Global Telecommunications Conference, 2002. GLOBECOM ’02*, 2002, vol. 1, pp. 178 – 182 vol.1.

[23] S. Bansal and M. Baker, “Observation-based Cooperation Enforcement in Ad hoc Networks,” *Research Report, cs.NI/0307012*, vol. 2, no. 1, pp. 1–10, Jul. 2003.

[24] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in *Sensor Network Protocols and Applications, 2003.*, Berkeley, CA, USA, 2003, pp. 113 – 127.

[25] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris, “Resiliency of wireless sensor networks: Definitions and analyses,” in *2010 IEEE 17th International Conference on Telecommunications (ICT)*, 2010, pp. 828 –835.

[26] J. Dong, R. Curtmola, and C. Nita-Rotaru, “Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks,” in *Proceedings of the second ACM conference on Wireless network security*, New York, NY, USA, 2009, pp. 111–122.

[27] D. Charles, K. Jain, and K. Lauter, “Signatures for Network Coding,” in *2006 40th Annual Conference on Information Sciences and Systems*, March, pp. 857–863.

[28] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, “An Efficient Signature-Based Scheme for Securing Network Coding Against Pollution Attacks,” in *IEEE INFOCOM 2008. The 27th Conference on Computer Communications*, April, pp. 1409–1417.

[29] M. N. Krohn, M. J. Freedman, and D. Mazieres, “On-the-fly verification of rateless erasure codes for efficient content distribution,” in *2004 IEEE Symposium on Security and Privacy, 2004. Proceedings*, May, pp. 226–240.

[30] C. Gkantsidis and P. R. Rodriguez, “Cooperative Security for Network Coding File Distribution,” in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April, pp. 1–13.

[31] A. Ababnah and B. Natarajan, “Optimal Control-Based Strategy for Sensor Deployment,” *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 41, no. 1, pp. 97–104, Jan.

[32] A. Sobeih, J. C. Hou, L.-C. Kung, N. Li, H. Zhang, W.-P. Chen, H. Tyan, and H. Lim, “J-Sim: a simulation and emulation environment for wireless sensor networks,” *IEEE Wireless Communications*, vol. 13, no. 4, pp. 104–119, Aug.

[33] Y. B. Reddy, “A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks,” in *Third International Conference on Sensor Technologies and Applications, 2009. SENSORCOMM ’09*, June, pp. 462–468.

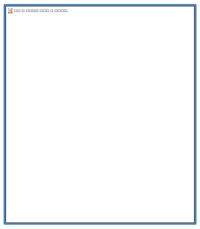
[34] Y. Ma, H. Cao, and J. Ma, “The intrusion detection method based on game theory in wireless sensor network,” in *2008 First IEEE International Conference on Ubi-Media Computing*, 2008, pp. 326–331.

[35] N. Iriawan, S. Astutik, and D. D. Prastyo, “Markov Chain Monte Carlo – Based Approaches for Modeling the Spatial Survival with Conditional Autoregressive (CAR) Frailty,” *International Journal of Computer Science and Network Security,*, vol. 10, no. 12, pp. 1–7, Dec. 2012.

[36] S. J. Godsill, “On the Relationship Between Markov Chain Monte Carlo Methods for Model Uncertainty,” *Journal of*

*Computational and Graphical Statistics*, vol. 10, no. 2, pp. 230–248, Jun. 2001.

**Muhammad Raisuddin Ahmed** currently serves as Lecturer (Teaching Fellow) at the Faculty of Information Sciences and Engineering, University of Canberra (UC), Australia. He was a distinguished member of the Board of directors of ITE&E Canberra Division, Engineers Australia in 2011. Besides, from March 2009 until July 2011, he was working as a Research officer and Project coordinator of BushLAN project at the Plasma research Laboratory, Research School of Physics and Engineering, at the Australian National University (ANU), Australia. During this time he was also an academic in the College of engineering and computer science at ANU from February 2010 till November 2011. He is pursuing his PhD at the UC, Australia. He has received Master of Engineering studies in Telecommunication and a Masters of Engineering Management degree from the University of Technology, Sydney (UTS), Australia. He obtained his Bachelor of Engineering (Hons) Electronics Majoring in Telecommunications degree from Multimedia University (MMU), Malaysia. His Research interest includes: Wireless Sensor Networks, Distributed Wireless Communication, Blind Source Separation, RF technologies, RFID implementation.



**Professor Xu Huang** has received the B.E. and M.E. degrees and Ph.D. in Electrical Engineering and Optical Engineering prior to 1989 and the second Ph.D. in Experimental Physics in the University of New South Wales, Australia in 1992. He has earned the Graduate Certificate in Higher Education in 2004 at the University of Canberra, Australia. He has been working on the areas of the telecommunications, cognitive radio, networking engineering, wireless communications, optical communications, and digital signal processing more than 30 years. Currently he is the Head of the Engineering at the Faculty of Information Sciences and Engineering, University of Canberra, Australia. He is the Course Conveners "Doctor of Philosophy," "Masters of Information Sciences (by research)," and "Master of Engineering." He has been a senior member of IEEE in Electronics and in Computer Society since 1989 and a Fellow of Institution of Engineering Australian (FIEAust), Chartered Professional Engineering (CPEng), a Member of Australian Institute of Physics. He is a member of the Executive Committee of the Australian and New Zealand Association for Engineering Education, a member of Committee of the Institution of Engineering Australia at Canberra Branch. Professor Huang is Committee Panel Member for various IEEE International Conferences such as IEEE IC3PP, IEEE NSS, etc. and he has published about two hundred papers in high level of the IEEE and other Journals and international conference; he has been awarded 9 patents in Australia.

**A/Prof. Hongyan Cui** has received the Ph.D. in School of Telecommunications Engineering in Beijing University of Posts and Telecommunications in 2006. She is engaged in communication network research and development work since 2000. She has been participated in two National 973 Projects, four 863 Projects, two National Nature Funds, a ministerial project, and a corporate-funded research project. She has published over 30 papers in the important journals / conferences, two books since 2003. She applied eight patents. She is the reviewer of the " Chinese Journal of Electronics"," Journal of Communications " ,"Journal of Beijing University of Posts and Telecommunications", "IEEE Networks Magazine SI", "Chaos" etc. She has trained 34 undergraduate students for graduation design,, and guided 31 Masters, in which 16 have graduated , and now she also assisting guided 3 doctoral students. Her research interest is future networks architecture, ESN, and Clustering.