CHAPTER 5

FUZZY GAME THEORY TRUST ASSOCIATIVITYBASED ROUTING TO MITIGATE NETWORK ATTACKS IN PERVERSIVE HEALTH MONITORING SYSTEMS

5.1 INTRODUCTION

Optimal routing is challenging in multihop networks. A routing protocol must ensure that a session has a route which satisfies Quality of Service (QoS) requirements (bandwidth, delay and jitter). Also, the protocol should ensure there is no network congestion by load balancing routes to use resources optimally. Devices which participate in a Mobile Adhoc NETworks (MANETs) are usually small with limited processing power, memory and storage. Bandwidth is shared by devices in an area through wireless communication. Also, increased network traffic results in more load on network nodes which thus leads to increased energy consumption (Patel et al., 2015). So, designing a technique that uses energy minimally and uniformly is a challenge.

Nodes cooperate with neighbours when their communication ranges are limited, to forward other’s packets thereby extending the network’s communication range overall. The scenario can be this: sensor nodes are deployed to sense temperature in a region. The sensed value is forwarded to a base station or powerful node. The information is meant offset a disastrous event.
A new routing protocol class called trust based routing emerged recently. These protocols have a routing part and trust model. Routing decisions are trust model based. Trust and reputation were used in settings to cope with uncertain interactions. Trust assesses risk associated with cooperating with others; and estimates how another is likely to fulfil commitments (El-Haleem & Ali 2011).

5.2 SECURE ROUTING PROTOCOL

MANET routing is a critical issue as nodes collaboration is a must for packet relay on behalf of others, and so a node is also a router. To ensure MANET security from attacks, a routing protocol has requirements it has to fulfill so that proper path functioning from source to destination is assured in the midst of malicious nodes Sadawarti & Gupta (2009). These are:

- Authorized nodes should perform route computation and discovery.
- Minimal exposure of network topology
- Detection of spoofed routing messages
- Detection of fabricated routing messages
- Detection of altered routing messages
- Avoiding formation of routing loops
- Prevent redirection of routes from shortest paths.

SRPs conforming to most requirements were developed recently. The protocols use varied cryptographic tools to protect different routing protocols vulnerabilities. Protocol touting for MANETs is divided into two categories:
- Proactive or table-driven routing protocols
- Reactive or on-demand routing protocols

Secure routing has a big role in MANET security due to a lack of fixed infrastructure. Conventional Internet routing protocols care not compatible with MANETs as they lack a clear defence. Though a design can ensure increased security using digital signature, CA, hop-by-hop control traffic validation, they are unsuitable for MANETs as mobile nodes lack computation power to perform costly operations (Ertaul & Ibrahim 2009).

SRP aims to create a Security Association (SA) between source and destination nodes. SA set starts through negotiating a shared key based on another’s public key. Then the key is used to encrypt/decrypt messages. Packets always carry an unencrypted routing path as no intermediate nodes knows anything about a shared key as it needs a current CA, an open environment.

Routing protocols were usually designed considering security. It was thought that all MANET nodes are trustworthy. But it is not so in large scale/dynamic MANETs. If a routing protocol is unprotected, the MANET becomes vulnerable to many security attacks. Due to MANET reactive routing protocols dominant status, security research was focused on them (Karlsson et al 2012).

For MANETs SRPs are extensions of current routing protocols. Security extensions are either cryptographic or trust-based. Trust and security are interrelated concepts. Using trust leads to enhanced network security.
5.3 HEALTH MONITORING SYSTEM

MANET networks comprise communicating devices which interconnect without any existing infrastructure, spontaneously. In-range devices communicate point-to-point. These devices are mobile generally. More people show interest in ad hoc networks. In addition to their growing military applications importance, their impact on business has also increased. Wide spread use of lightweight and nominally priced mobile devices include mobile phones and Pocket PCs which now have embedded WiFi (IEEE 802.11) Bluetooth and network adapters ensuring city-wide MANET creations spontaneously. Such networks are the infrastructure of applications like advertisements, emergency and health-care systems, groupware, customer to customer applications and gaming (Hogie et al 2006).

Now we have advanced health care applications for ad-hoc networks. The ability to improve health care telemetry through use of wearable mini wireless sensors will deeply impact medical practice. As regards efficiency, small portable wireless devices have a big role in health care providing all needed support for patients. Wireless health care monitors/equipment available include pulse Oximeters, blood pressure monitors, Wireless Electrocardiogram (ECG) System, maternal uterine and fetal heart rate monitors and Electrocardiographs (EKGs). In disaster recovery or casualty, doctors affix sensors on patients and monitor results through laptops and PDAs (Abid et al 2014).

Data integrity, availability and security are emphasized in health care. Currently, private and public key security is implemented in data of adhoc networks. Packet loss may be compromised due to mobility and congestion. Multiple doctors/nurses are now able to retrieve patient data using multicast semantics support on a network layer. Due to patients being mobile,
doctors route changes quickly, necessitating the availability of energy efficient and multi-hop routing protocols.

Advances in wireless communications, semiconductors and physiological sensing have given rise to small, lightweight and limited power, intelligent monitoring devices are due to advances in wireless communication, physiological sensing and semiconductors. Such devices are integrated in a Wireless Body Area Network (WBAN), a technology which monitors health. Aging populations in developed countries and rising health costs triggered development of new technology-driven enhancements for present day health care practices. Today, a healthcare system is focused on early detection/prevention of chronic diseases ensuring an inexpensive but smart way to manage patient care to alleviate suffering from age-related perennial ailments like heart disease which needs continued, long-term monitoring instead of temporary assessments (Murthy & Rao 2013).

Now, wearable health monitoring system are easy to use and consist of tiny remote sensors, placed on a body strategically, creating a WBAN to monitor vital parameters and ensure real-time feedback both to user and medics. They alert medical personnel about life-threatening changes when integrated into telemedicine. Wearable systems are also used for patient health monitoring in ambulatory settings.

MANETs nodes communicate through a multi-hop method. A node forwards a packet to destination through an intermediate node with every node acting as both end system and router. As E-Health Monitoring System (EHMS) services are information based, better use of information can make services integrated and enhance patient safety and accountability. A EHMS challenge is find the best routing protocol which ensures transmission of data from a node to another quickly (Morshed et al 2010).
Wearable health monitoring systems permit individuals to monitor changes in her/his vital signs providing feedback to maintain optimal health. Such systems alert medical personnel when life-threatening changes occur when inbuilt into a telemedical system. Patients also benefit from continuous long-term monitoring; ensuring optimal maintenance of chronic conditions, or be supervised during recovery from an illness or post surgical procedures (Milenkovic et al 2006).

Long-term health monitoring captures physiological signals diurnal and circadian variations. Such variations are very good recovery indicators for cardiac patients after myocardial infarctions. Long-term monitoring ensures adherence to treatment guidelines (regular cardiovascular exercise) or monitor drug therapy effect. Other patients also benefit from such systems; monitors can be used during rehabilitation after hip/knee surgeries, stroke rehabilitation, or in brain trauma rehabilitation.

"Intelligent Mobile Health Monitoring System (IMHMS)" a bio-sensor based mobile health monitoring system uses Wearable Wireless Body/Personal Area Network to collect patients data, mining data and intelligently predicts patient’s health status in addition to ensuring feedback to patients through mobile devices (Shahriyar et al., 2010). Patients will more than willing to participate in such a health care process if they can access their health information through their mobile devices, anywhere, any time. Till date mobile health care has no related automated medical server.

Many specialists are needed for continuous monitoring and to maintain a server. Many specialists being available always is an impossibility. Also specialist with limited knowledge might provide incorrect prescriptions as in third world countries. Use of an Intelligent Medical Server (IMS) in mobile health care can help health care specialists. As voluminous medical data is handled by servers, they have to mine and analyze data.
The IMHMS contains three components. They are Wearable Body Sensor Network (WBSN), Patients Personal Home Server (PPHS) and IMS. Tele-health care repositories capture patient data via SMS, phones and emails with locations, patient-ID and disease-code. A collaborative process, it communicates synchronous messages, audio/video conference records and sensor transmitted automation transactions. Patients dialogue their status with medical experts at their choice and even request additional services. A workflow system controls and presents patient data based on individual’s data access rights. Earlier telemedicine systems were point to point in that a rural health centre was attached to a city hospital and patient’s requests were meant for only that hospital’s doctors (Sarkar et al. 2011). Taking into consideration the volume of common ailment in East Asia with specific reference to India to support a telemedicine program, a minimum basic setup at layer 1 PHC should comprise equipment including Personal Computer and Printer, Internet Protocol enabled Video conferencing Kit and clinical devices, Telemedicine operating system supported software and a server software, Digital ECG device, A3 Scanner, Digital Microscope and camera, Tele-auto scope for remote listening of patient heart beat, Glucometer for blood sugar estimation, Haemogramanalyzer for blood count and blood film, Modem/router/Wi-Fi /Manet etc.

5.4 METHODOLOGY

Fuzzy theory is a technique for distributed manufacturing system’s quality management which attracted the attention of both academics and industry. This work describes both Fuzzy game theory based model and use of dwelling selection. Game theory development studies include decision making in conflicts and also in cooperation. Game theory is a mathematical process to choose an optimal strategy (Medineckiene et al., 2011). Game theory solves engineering problems in decision-making.
Game theory gives mathematical tools and models to investigate multi person strategic decision making in which players or Decision Makers (DM) can compete for limited/shared resources. Security games study is a special case of interaction between malicious attackers and defenders. Security games and solutions are the foundation for decision making and algorithm development which also predict attacker behaviour. Based on information with DMs, action space and DMs goal, security games vary from simple deterministic to complex stochastic and limited information formulations applicable to security problems in varied areas from privacy to intrusion detection and cryptography in computer, wireless and vehicular networks.

An analytical tool, Game theory helps researchers design computer network security protocols. This mathematical tool analyses and models new security problem (Manshaei et al., 2011). Also, the defender has a deeper understanding of an attacker's strategies through equilibrium analysis of a security game as also the potential attack risks involved. Consider

$$\mu_A = \begin{cases} 
0, & \text{when } A \leq a_1, \\
2 \times \left( \frac{A-a_1}{a_3-a_1} \right)^2, & \text{when } a_1 \leq A \leq a_2, \\
1 - 2 \times \left( \frac{A-a_2}{a_3-a_1} \right)^2, & \text{when } a_2 \leq A \leq a_3, \\
1, & \text{when } A \geq a_3,
\end{cases}$$

Where $a_1$, $a_2$, $a_3$ are subjectively selected values. Dependency function is a description of dependence of dependency value’s ($\mu$) from options of values ($x$), based on the parameters models $\mu(x, p)$.

Uncertain network status $us$ is considered a factor in routing decisions (Dai et al., 2009) by fuzzy routing protocols. A fuzzy routing
algorithm monitors routing congestion status and feeds network status to a fuzzy logic controller to help make a best routing decision. Membership functions in the work include number of successful deliveries, memory use and computed trust. Trust, a natural fuzzy concept poses as a fuzzy constraint on trusted routing decision-making, so that different nodes ensure diverse routings on same nodes, i.e., different nodes have different/opposite trust evaluations for same node. A node calculates trust value for neighbours and maintains it in a neighbour route table based on a fuzzy model. Minimal trust values are due to a neighbouring node’s malicious behaviour instead of legitimate behaviour.

Members taking expected action $a^*_{i,(L+2)\pi(L+2)}$ in choosing cooperative behaviour ensure a higher trust level (trust-preferential strategy) in themselves in large scale MANETs. Nodes continue to receive high-level cooperative services in new area through their high trust level (Wang et al., 2013) even when network topology changes suddenly. But, optimum actions refer to a strategy of receiving the highest payoff for players in game theory.

A trust model suits a system’s differing situations. Nodes may join/leave a network anytime in open MANETs. Some nodes know each other even before joining a network (Li et al., 2005). Pre-shared knowledge in addition to direct interaction network experience is important for nodes to implement trust evaluation. So a trust model should have considerable accountable experience.

### 5.5 EXPERIMENTAL RESULTS

Simulations were conducted for varying mobility speed using random way point mode. Nodes in the network are selected randomly to act maliciously by either control packet dropping or packet dropping. The
maliciousness in the network is varied 10%, 20% and 30%. Fifty nodes were used in the simulation with the range of each node being 250 m and the size of the network being 2000 sqm. ABR and the proposed FGT2-ABR are simulated in these scenarios and its performance with regard to the number of hop count, end to end delay and packet delivery ratio is evaluated. Table 5.2 and Figure 5.1 shows the number of hops to destination when ABR routing is used for different number of malicious nodes.

![Figure 5.1 Number of hops to destination for ABR](image)

It is seen from Figure 5.1 that the number of hops to destination for ABR increases with the increase in mobility speed and maliciousness due to the frequent packet drops and lost packets. It is seen that the mobility has great impact on the number of hops to destination, as the mobility increases from 30 to 90 kmph the number of hops to destination increases by 10.71% to 53.57% when compared with 10 kmph speed in a non-maliciousness network. Figure 5.2 show the number of hops to destination.
It is seen from Figure 5.2 that the number of hops to destination for the proposed FGT2-ABR increases with the increase in mobility speeds and maliciousness. As mobility increases from 30 to 90 kmph, the number of hops to destination increases by 14.29 to 50% when compared with 10 kmph speed in a non-maliciousness network. The Number of hops to destination increases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR on an average has similar number of hops to destination when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves decreased number of hops to destination by 6.06 to 11.76% to 3.4% than ABR. Table 5.1 and Figure 5.3 shows the end to end delay in seconds for various scenarios.

It is observed from Table 5.1 that the proposed FGT2-ABR consistently reduces delay when compared with ABR. It is also seen that as the maliciousness increases, the delay is much lower for the proposed FGT2-ABR. It has been perceived that the end to end delay for the proposed FGT2-ABR decreased in the range of 0.89% to 2.99% for a non-malicious network.
When compared to ABR, the proposed FGT2-ABR has lower end to end delay in the range of 2.93% to 3.11% when the network has 20% malicious nodes.

Table 5.1 Comparison of ABR and FGT2-ABR for End to End delay (%)

<table>
<thead>
<tr>
<th>Node Mobility in Kmph</th>
<th>No maliciousness</th>
<th>10% maliciousness</th>
<th>20% maliciousness</th>
<th>30% maliciousness</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1.3527</td>
<td>1.9625</td>
<td>2.9268</td>
<td>3.0996</td>
</tr>
<tr>
<td>30</td>
<td>1.9934</td>
<td>2.7231</td>
<td>3.0261</td>
<td>3.123</td>
</tr>
<tr>
<td>50</td>
<td>1.1628</td>
<td>2.8245</td>
<td>3.0544</td>
<td>3.3296</td>
</tr>
<tr>
<td>70</td>
<td>2.9851</td>
<td>2.9169</td>
<td>3.1088</td>
<td>3.4537</td>
</tr>
<tr>
<td>90</td>
<td>0.8889</td>
<td>2.936</td>
<td>3.0933</td>
<td>3.3931</td>
</tr>
</tbody>
</table>

Figure 5.3 End to End delay for ABR

From Figure 5.3 that the end to end delays for ABR increases with the increase in mobility speed and maliciousness. It is seen that the mobility has great impact on the end to end delay, as the mobility increases from 30 to 90 kmph the end to end delay increases by 7.99% to 52.52% when compared
with 10 kmph speed in a non-maliciousness network. The delay increases significantly more as the increase in maliciousness in the network. Table 5.5 and Figure 5.4 show the end to end delay for the proposed technique.

![Figure 5.4 End to End delay for FGT2-ABR in second](image)

It is seen from Figure 5.4 that the end to end delay for the proposed FGT2-ABR increases with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph the end to end delay increases by 5.75% to 51.82% when compared with 10 kmph speed in a non-maliciousness network. The delay increases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR has more end to end delay in the range of 0.89% to 3.03% when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves decreased delay of 3.05% to 3.4% than ABR. Figure 5.5 and Table 5.6 shows the Packet Delivery Ratio (PDR) for ABR
It is observed from Figure 5.5 that the packet delivery ratio for ABR decreases with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph the packet delivery ratio decreases by 2.13% to 9.79% when compared with 10 kmph speed in a non-maliciousness network. The packet delivery ratio decreases significantly more in the increase in maliciousness in the network. Similarly Table 5.7 and Figure 5.6 show the PDR of the proposed technique.
Figure 5.6 Packet delivery ratio for FGT2-ABR

It is observed from Figure 5.6 that the packet delivery ratio for proposed FGT2-ABR decreases with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph the packet delivery ratio decreases by 2.15% to 10.36% when compared with 10 kmph speed in a non-maliciousness network. The packet delivery ratio decreases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR has better packet delivery ratio in the range of 6.94% to 7.61% when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves higher packet delivery ratio of 7.61% to 8.18% than ABR.
Table 5.2 Comparison of ABR and FGT2-ABR for packet ratio delivery (%)

<table>
<thead>
<tr>
<th>Node Mobility in Kmph</th>
<th>No maliciousness</th>
<th>10% maliciousness</th>
<th>20% maliciousness</th>
<th>30% maliciousness</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>7.33</td>
<td>8.96</td>
<td>8.34</td>
<td>7.86</td>
</tr>
<tr>
<td>30</td>
<td>7.02</td>
<td>8.78</td>
<td>8.32</td>
<td>7.85</td>
</tr>
<tr>
<td>50</td>
<td>6.74</td>
<td>8.76</td>
<td>8.27</td>
<td>7.69</td>
</tr>
<tr>
<td>70</td>
<td>6.72</td>
<td>8.51</td>
<td>8.05</td>
<td>7.45</td>
</tr>
<tr>
<td>90</td>
<td>6.71</td>
<td>8.5</td>
<td>7.91</td>
<td>7.33</td>
</tr>
</tbody>
</table>

It is observed from Table 5.2 that the proposed FGT2-ABR consistently increases packet delivery ratio when compared with ABR. It is also seen that as the maliciousness increases, the packet delivery ratio is higher for the proposed FGT2-ABR than ABR.

It has been perceived that the packet delivery ratio for the proposed FGT2-ABR increased in the range of 6.71% to 7.33% for a non-malicious network. When compared to ABR, the proposed FGT2-ABR has higher packet delivery ratio in the range of 7.91% to 8.34% when the network has 20% malicious nodes.
Table 5.3 Summary of results

<table>
<thead>
<tr>
<th>Node mobility in Kmph</th>
<th>ABR</th>
<th>ABR - with 20% maliciousness</th>
<th>Fuzzy Trust ABR</th>
<th>Fuzzy Trust ABR - with 20% maliciousness</th>
<th>FGT2-ABR with 20% maliciousness</th>
<th>FGT2-ABR</th>
<th>Cooper et al., 20% maliciousnodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet Delivery Ratio</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0.9027</td>
<td>0.7593</td>
<td>0.935</td>
<td>0.7903</td>
<td>0.9715</td>
<td>0.8254</td>
<td>0.7713</td>
</tr>
<tr>
<td>30</td>
<td>0.8948</td>
<td>0.7526</td>
<td>0.9498</td>
<td>0.7835</td>
<td>0.9599</td>
<td>0.8179</td>
<td>0.7688</td>
</tr>
<tr>
<td>50</td>
<td>0.8642</td>
<td>0.7269</td>
<td>0.9093</td>
<td>0.7444</td>
<td>0.9245</td>
<td>0.7896</td>
<td>0.7597</td>
</tr>
<tr>
<td>70</td>
<td>0.8321</td>
<td>0.6998</td>
<td>0.8519</td>
<td>0.7182</td>
<td>0.89</td>
<td>0.7585</td>
<td>0.7035</td>
</tr>
<tr>
<td>90</td>
<td>0.8144</td>
<td>0.685</td>
<td>0.8621</td>
<td>0.7389</td>
<td>0.8709</td>
<td>0.7414</td>
<td>0.69</td>
</tr>
<tr>
<td>End to End Delay in sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0.0514</td>
<td>0.0624</td>
<td>0.0516</td>
<td>0.062</td>
<td>0.0521</td>
<td>0.0606</td>
<td>0.0685</td>
</tr>
<tr>
<td>30</td>
<td>0.0608</td>
<td>0.0738</td>
<td>0.0602</td>
<td>0.0736</td>
<td>0.0596</td>
<td>0.0716</td>
<td>0.0829</td>
</tr>
<tr>
<td>50</td>
<td>0.0684</td>
<td>0.0831</td>
<td>0.0688</td>
<td>0.0808</td>
<td>0.0692</td>
<td>0.0806</td>
<td>0.0909</td>
</tr>
<tr>
<td>70</td>
<td>0.0726</td>
<td>0.0882</td>
<td>0.0733</td>
<td>0.0873</td>
<td>0.0748</td>
<td>0.0855</td>
<td>0.0968</td>
</tr>
<tr>
<td>90</td>
<td>0.0784</td>
<td>0.0952</td>
<td>0.0789</td>
<td>0.0944</td>
<td>0.0791</td>
<td>0.0923</td>
<td>0.1059</td>
</tr>
</tbody>
</table>

Table 5.3 shows the summary of results which includes ABR, fuzzy Trust with ABR and Fuzzy Game Theory Trust with malicious of 10%, 20% and 30%. Results prove that the Fuzzy Game Theory Trust performs in a
better way than other two techniques. The proposed technique improves the PDR over 3% compared to work proposed by Cooper et al (2013).

5.6 CONCLUSION

MANETs comprise wireless nodes exchanging data among themselves dynamically without a fixed base station or wired backbone network. MANET nodes are distinguishable by their limited power, processing and memory resources and their high mobility. This work uses a Fuzzy game theory for route selection. Membership functions are number of successful deliveries, memory use and computed trust in this work. Trust is dependent on neighbourhood trust and recommendation based trust.

Experiments in varied scenarios using ABR and the new method were conducted. Results revealed that the new approach’s improved performance on packet delivery ratio. The new FGT2-ABR had improved packet delivery ratio which ranged between 6.94% and 7.61% when a network had no malicious nodes. In a network with 30% malicious nodes, the new FGT2-ABR achieved higher packet delivery ratio which ranged between 7.61% and 8.18% compared to ABR. More research is necessary to reduce end to end delay which was slightly higher in the new technique.