Detection and Isolation of Wormholes in Mobile Ad-hoc Networks Using Localization Information

Govand Salih Kadir[1] and Ihsan Alshahib Lami[2]
(Corresponding author: Govand Salih Kadir)
Department of Computer Science and Engineering, University of Kurdistan-Hewler[1]
30M Avenue, Erbil, Iraq
Department of Applied Computing, University of Buckingham[2]
Yeomanry House, Hunter St, Buckingham MK18 1EG, United Kingdom
(Email: g.kadir@ukh.edu.krd)
(Received Aug. 25, 2017; revised and accepted Nov. 28, 2017)

Abstract

Mobile Ad-hoc Networks rely on participating nodes to conduct routing duties and forwarding data packets between nodes, mainly due to their limited transmission capabilities. Routing protocols intend to minimize the exchange of information to reduce overhead, which in result leads to lack of knowledge about others beyond the transmission range of a selected path. This creates a perfect environment for wormholes (WHs) to direct the route discovery through themselves and harm the network. This paper proposes an enhancement to the SIMAN (Smart Identification of MANET Nodes) algorithm that facilitates location sharing of nodes within the discovered path and allows source nodes to reject the path if the distance between any two nodes exceeds the transmission capability of the wireless device. Nodes are authenticated through the original identity sharing mechanisms of the SIMAN algorithm applied during the RREP process of the AODV routing protocol.

Keywords: Aodv; Manet; Siman; Wormhole

1 Introduction

MANET emerged as a promising technology offers infrastructure-less networks that do not require central management entities. Current wireless devices, like Smart-phones, can use MANET to create/join a network, exchange data, and quickly disconnect without prior notification or permission. Nodes in MANET take the central role of finding the possible paths between any two or more nodes separated from each other via some distance within the network. These nodes are wireless devices with limited transmission and power capabilities that can sense the neighbors inside their transmission range only [6, 7]. Therefore, to find a path to a specific destination, each node relies on each other to forward packets. Moreover, routing protocols are designed to avoid overhead caused by additional processes that provide further information about the vicinity to preserve the limited resources of nodes inside the network. As a result, it creates a suitable environment for malicious nodes to expose and launch attacks. Wormholes (WH) are one of the dangerous attacks that is hard to detect and prevent due to limited knowledge about the physical location of nodes inside the network. Two or more malicious nodes can cooperate and use a high-speed link between them to win the route discovery and subsequently harm the network [15].

This paper proposes an enhancement to a previously designed algorithm called SIMAN [5].Which is designed to share knowledge about nodes identity inside the discovered path using AODV routing protocol RREP message. This is achieved by calculating two values from Friend nodes IP address (nodes who are known to each other during the initial network set-up and have an IP address with a prime number host part) and then using these two values by any node inside the transmission path to get a list of addresses for previous nodes inside the route to destination. Furthermore, the enhancement replaces nodes reliance on routing tables to retrieve the previous and next nodes address using a mathematical formula to forward packets during data transmission. This concept provides an abstract authentication of nodes inside the transmission path. Additionally, it is used to prevent newly joined unknown nodes called (Bridging nodes) from altering any information passed through the RREP message because they will not be aware of the algorithms existence.

The current enhancement uses location information, obtained from GPS-enabled devices like Smart-phones, to measure the distance between nodes and detect any abnormal distances. Every Friend node attach its coordinates to RREP message and passed it all the way back to the source node. The source node then accepts the discovered route if the distance between nodes is less than the threshold defined according to maximum transmission

characteristics of the wireless environment. Additionally, three Friend nodes cooperate to determine Bridging node coordinates and attach it to the RREP message on their behalf. If the distance between any two nodes inside the discovered path is greater than a pre-determined threshold, the source then rejects the path and start a new route discovery.

The rest of this paper organized as follows: Section 2 explores the recent work done that involves the usage of localization information to improve routing protocol performance and ways of WH attacks prevention. Section 3 explains the proposed algorithm design and Section 4 details the implementation of the algorithm using Riverbed Simulation software. Section 5 examines the simulation results of various scenarios in comparison to AODV routing protocol. Finally, we conclude the achievements obtained through this enhancement and identify the future use of this method in security protocols in Section 6.

2 Literature Review

MANET is restricted by the limited information shared among nodes about the physical location of others inside the network. Sharing such information improves the performance and provides better protection against malicious nodes. Researchers used various approaches toward this goal, in this section, we explore some of these methods used for this purpose.

The Geographical AODV (GeoAODV) is an improvement of the LAR protocol, which uses directed flooding technique with AODV routing protocols. The physical location of nodes is used to reduce the amount of broadcasted route requests messages aimed at a destination node by defining the request zone as an isosceles triangle. Nodes inside the request zone process RREQ messages and share location information, while others outside the zone discard the messages [1].

The same concept of requested and expected zones is used in another research to limit the search area during route discovery. A list added to the route request message, which contains a fourth Nominated Neighbor to rebroadcast. The algorithm partitions the radio transmission range into four zones and restricts the path discovery area to the expected zone. Then chooses one node per zone to forward the RREQ messages [3]. The proposed solutions reduce the route discovery traffic toward saving resources. However, it does not consider applying the zone restriction might lead to overhead and deny essential nodes that provide better alternative paths for data transmission.

In another research work, an On-demand Routing with Coordinates Awareness (ORCA) protocol uses the distance measurement for broadcasting route request messages. The node broadcast the packets to selected neighbors (called relays) using the shortest Euclidean distance to four points in its transmission range. Based on this calculation, the algorithm selects the neighbors closest to these polar points to flood the route requests [17]. The algorithm relies on Hello message to exchange the coordinates and identifiers of a node and its neighbors, which results in creating extra processing that causes overhead, especially in large networks.

Another recent approach, the distance measurement between nodes was used to improve the route stability affected by node mobility. Nodes typically use the RSSI method to quantify the mobility of its neighbors and formulate a method to find the coordinates of nodes when GPS devices do not exist. The method is used as a mobility metric to obtain routes that stay longer, which improves the performance [12]. This concept works better if the distance list was attached to the RREP message, rather than the RREQ, to avoid additional loads on nodes that are not a part of the established path.

The distance measurement between nodes used in another research to confirms the location of neighboring nodes securely in wireless sensor networks [14]. The neighbor verification protocol identifies nodes as true neighbors if the link between four nodes with known distances forms a convex quadrilateral. These nodes exchange location information through what is called a neighbor table, and they use encryption to prevent alteration. The disadvantage of this protocol is the number of operations conducted to exchange data and confirm each other, which creates overhead in addition to the inconsistencies that occur due to 4-clique tests.

Additionally, location information is used to detect and prevent attacks from malicious nodes like WHs. The nodes inside the discovered route measure the distance to the neighbors and share it with others inside the path [2]. The concept of this algorithm can provide knowledge beyond the neighbors of a node, and it requires a mechanism to hide the implementation from WHs because they can defeat the algorithm by merely sharing the wrong distance between them.

Likewise, another technique, called AODV With Wormhole Detection and Prevention (AODVWWDP), is used for WH elimination. This method uses location, hop count and neighboring nodes in a route selection process suggested by AODV. Every node makes sure that the path from neighbor to the node next to neighbor is WH free, by examining different paths and determining if the hop count is greater than a maximum hop count that was calculated earlier [13]. It is not clear in the research how the location helps toward eliminating open attacks from WH nodes, as they act like normal nodes and that can be hard to detect. Furthermore, several hop count calculations cause much overhead that consumes resources. Moreover, it is not clear how the node identifies the node next to neighbors without exchanging further information.

Similarly, the location information was used in another research to detect and prevent WHs by allowing nodes to share their distances from the next node and the next one beyond. This process map nodes inside the path so that the network provide knowledge about the distance

between all nodes [16]. In theory, the algorithm can provide knowledge about all node locations, even those beyond the neighbors, but there is no guarantee that the WHs will not alter this information, which can be a big problem because of a lack of authentication authority.

Another protocol called the distance bounding protocol checks the proximity of two-hop neighbors to verify the physical presence of the node beyond its known neighbors. The round-trip-time for multi-cryptographic challenge-response pairs are used to obtain the upper bound of physical location between two nodes [9]. As discussed earlier, sharing knowledge of nodes beyond its neighbors is crucial to improving the performance of the network, but key-based security solutions used to exchange information adds extra processing that causes overhead and consumes node resources.

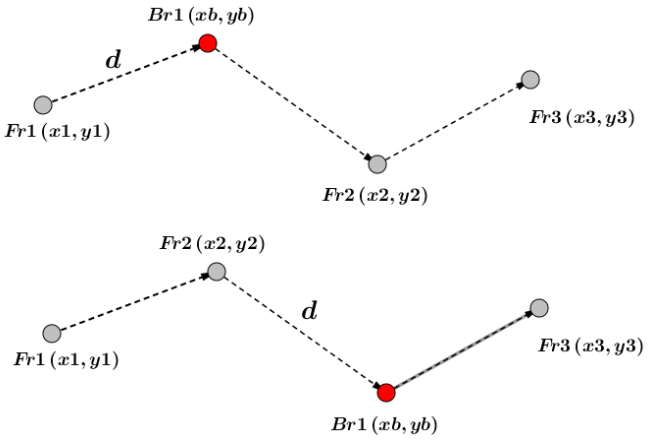

Figure 1: The sequence of friend and bridging nodes in the RREP process

3 Proposed Algorithm

The proposed algorithm is an enhancement of the original SIMAN algorithm, which uses two values generated from the IP addresses of the nodes inside the discovered path that is forwarded using RREP messages. These two values help to share knowledge about nodes identity inside the transmission path. The enhancement adds an extra field to the RREP message that holds a list, which contains the coordinates of the node in 2D obtained from a GPS device.

Each Friend node attaches its coordinates to the extra field added to RREP message, whereas Bridging nodes (earlier assigned prime ID by previous Friend nodes) are not involved in this process. Instead, Friend nodes cooperate to find the coordinates of the bridging node. Once the source node receives the RREP message, it uses the list of coordinates to measure the distance between nodes inside the discovered path and rejects the route if the distance exceeds the wireless transmission threshold. The algorithm is used to detect and isolate WH attacks initiated by malicious nodes hiding their location to take over the transmission path and harm the network. The measurement procedure, which is categorized according to the Friend and Bridging node topology layout, will be explained next.

3.1 Coordinate Measurement

1) If the procedure is between two Friend nodes (Fr), then the calculation will be a simple distance measurement between two points using the coordinate of the Friend attached to RREP.

2) If one of the nodes is a Bridge (Br), then the process requires the cooperation of three neighboring Friend nodes to calculate the coordinates of the Bridging node. The location of the Bridging node creates two different sequences: $\mathrm{Fr1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr3}$ and $\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3}$ as shown in Figure 1. Two different calculation tracks are used for different node

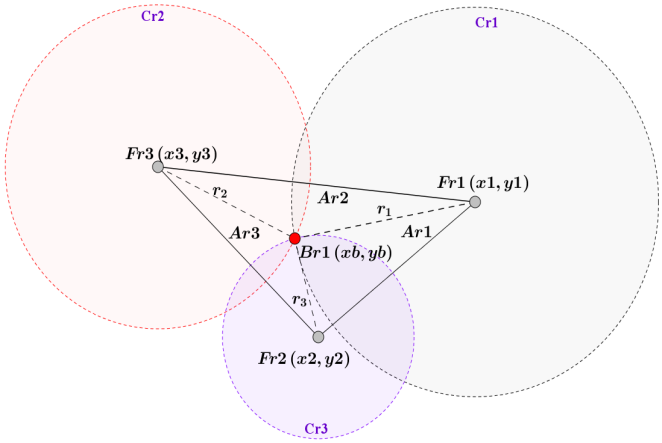

Figure 2: Three-circle intersection used to calculate bridging node location

sequences based on the location of the bridge node Br1 that can be inside or outside the triangle (Fr1, Fr2 and Fr3) as illustrated in Figure 2.

First track: If the Bridging node is located inside the triangle (Fr1, Fr2 and Fr3), then the intersection of the three circles theory will be used to calculate the coordinates (radical centre) [10]. Afterword, the resulting coordinates will be used to calculate the area of the three triangles (Ar1, Ar2 and Ar3). The sum of these areas should be equal to the area of the triangle (Fr1, Fr2 and Fr3) using the Pythagorean Theorem. The coordinates of the bridging node calculated using Equations (1) and (2) for the intersection of the three circles (Trilateration Estimation) [11]. Lets assume that:

$$A = ({y_3}^2 - {y_2}^2), B = ({x_3}^2 - {x_2}^2), C = ({r_2}^2 - {r_3}^2)$$

$$D = ({y_2}^2 - {y_1}^2), E = ({x_2}^2 - {x_1}^2), F = ({r_1}^2 - {r_2}^2)$$

Then

$$x_b = \frac{y_m[A+B+C] - y_n[D+E+F]}{2[x_m * y_n - x_n * y_m]} \quad (1)$$

and

$$A' = ({x_3}^2 - {x_2}^2), B' = ({y_3}^2 - {y_2}^2)$$

$$D' = ({x_2}^2 - {x_1}^2), E' = ({y_2}^2 - {y_1}^2)$$

Then

$$y_b = \frac{x_m[A'+B'+C] - x_n[D'+E'+F']}{2[y_m * x_n - y_n * x_m]} \quad (2)$$

The coordinate values then used to find the area of the three inner triangles (Fr1, Br1 and Fr2), (Fr1, Br1 and Fr3) and (Fr2, Br1 and Fr3) which is calculated using the determinant of three points (shoelace formula) as in Equation (3).

$$Tr_{area} = \frac{|x_1y_2 + x_2y_3 - x_3y_1 - x_2y_1 - x_3y_2 - x_2y_3|}{2} \quad (3)$$

The sum of these areas should equal the area of the main triangle (Fr1, Fr2 and Fr3) that contains them as in Equation (4).

$$Area_{main} = Ar_1 + Ar_2 + Ar_3 \quad (4)$$

Second track: Considering the two node sequences explained earlier as Fr1 → Fr2 → Br1 → Fr3 and Fr1 → Br1 → Fr2 → Fr3. The distance between the two outer Friend nodes (Fr1 and Fr3) represents the radius of two circles that intersect at two points. One of these two points represents the correct coordinates of the Bridging node as seen in Figure 3.

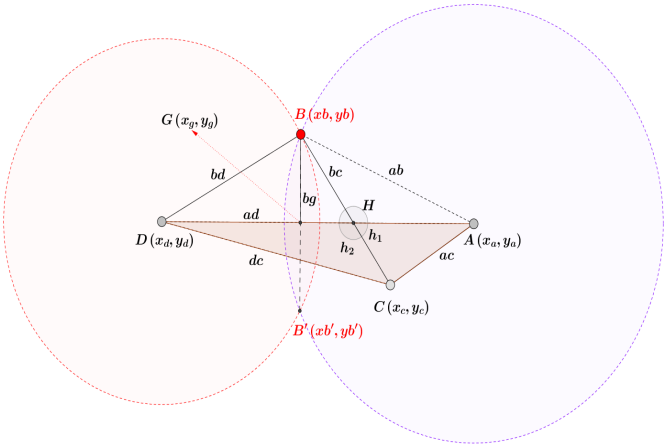

Figure 3: The distance between nodes (A, B and A, C) represents the radius of two circles

The following mathematical procedure will be used to find the actual coordinates of node B.

- The rules of sine and cosine used to derive the formulas used to find the length of the radius of the two circles as in Equations (5) and (6).

Law of Sine:

$$\frac{\bar{cd}}{\sin A} = \frac{\bar{ad}}{\sin C} = \frac{\bar{ac}}{\sin D} \quad (5)$$

Law of Cosine:

$$\bar{cd}^2 = \bar{ad}^2 + \bar{ac}^2 - 2 * \bar{ad} * \bar{ac} * \cos A \quad (6)$$

$$\bar{ac}^2 = \bar{ad}^2 + \bar{cd}^2 - 2 * \bar{ad} * \bar{cd} * \cos D$$

$$\bar{ad}^2 = \bar{cd}^2 + \bar{ac}^2 - 2 * \bar{cd} * \bar{ac} * \cos C$$

- The two radii are then used to calculate the intersection points B and B' of the radical line as in Equations (7) and (8).

$$x_b = x_g \pm \frac{\bar{bg}(y_d - y_a)}{2 * \bar{ad}} \quad (7)$$

$$y_b = y_g \pm \frac{\bar{bg}(x_d - x_a)}{2 * \bar{ad}} \quad (8)$$

- Finally, two different methods used to find the area of the triangle ABD.
  - The first method applies Heron's formula, seen in Equation (9).
    Assuming:
    $M = (\bar{ab} + \bar{ad} + \bar{bd}), N = (-\bar{ab} + \bar{ad} + \bar{bd}),$
    $P = (\bar{ab} - \bar{ad} + \bar{bd})\ and\ Q = (\bar{ab} + \bar{ad} - \bar{bd})$

$$Area = \frac{\sqrt{M * N * P * Q}}{4} \quad (9)$$

  - The second method applies the shoelace formula previously explained in Equation (3), and the result of one of the two points B and B' should yield an equal area as in Equation (10).

$$Area_{(Sides)} = Area_{(Coordinates)} \quad (10)$$

3) It is possible for two consecutive Bridging nodes to come one after another inside the path. The Friend node located after them can detect this, by comparing the hop count with the factor list items. The coordinate measurement for this case is accomplished in two stages. First, by computing the first Bridging node coordinates and then by using the discovered values for the other Bridging node.

4) Lastly, a particular case in which the path between the source and destination contains only two Bridging nodes, and as explained before the coordinates measurement require three Friend nodes. Therefore, when the Source node discovers this case, it creates a false RREQ to one of its neighboring Friend nodes. Once the source node receives the RREP back, it retrieves the coordinates of the Friend node and uses it to compute the coordinates of the Bridging nodes, using the previously explained procedure.

3.2 The Route Discovery

1) RREQ process: During the initial route discovery, the RREQ procedure is the same as in AODV routing protocol. Later when the source receives the RREP, if it detects an unusual distance between two nodes during the measurement process, then it rejects the route and starts a new route discovery.

   This procedure requires a mechanism to prevent the RREQ from following the same path by informing the Friend nodes inside the path to reject packets forwarded to them from nodes with surpassed distance. Therefore, two extra fields added to the RREQ message. The first field is called the S-list, which contains the list of rejected nodes. The second field is called the S-Flag, which is used to inform the other Friend nodes to distinguish it from initial RREQ.

   Once the RREQ is broadcasted, Friend nodes check the S-Flag field, and if it is set, then the node compares the address inside the S-list with preceding node. If a match is found, then it discard the packet otherwise, rebroadcast the RREQ.

2) RREP process: In this process, an extra field is added to the message format to hold the list of coordinates.

   - The destination node starts the process, by adding its coordinates and forward the RREP message to the previous node. Every Friend node receives the RREP repeat the same process as in Figure 4(1).
   - Bridging nodes are not aware of the algorithm, so they use AODV to process the RREP message shown in Figure 4(2).
   - When a Friend node receives the message from a Bridging node, it first checks the number of Friend nodes, preceding the Bridging node:
     - If there was two, then it starts the calculation using (Fr1 → Br1 → Fr2 → Fr3) otherwise, forwards this task to the next Friend node as in Figure 4(3).
     - If there was no other Friend node (i.e. The Friend node itself is the source), then it sends a special RREQ to another neighboring Friend node to get additional coordinates, which is required to measure between coordinates using the sequence (Fr1 → Fr2 → Br1 → Fr3) as in Figure 4(4).

   Assuming there were two Friend nodes before the Bridging node, then the next step is to check for the number of Bridging nodes by comparing the hop count with the factor list items [4]. If they were equal, then the one-step coordinate calculation is used. Otherwise, it uses the two-step procedure as seen in Figure 4(5).

   - If a Friend node received the RREP message and found that a Bridging node is without coordinates, then it will process it using (Fr1 → Fr2 → Br1 → Fr3) as in Figure 4(6).
   - This procedure continues until the RREP reaches the source node, which starts the distance measurement between nodes as seen in Figure 4(7).
   - If the distance between any two nodes exceeds the wireless transmission capability of devices, then the route is rejected, and the address of the nodes added to S-list of the RREQ. Otherwise, the route is accepted, and the source starts data transmission.

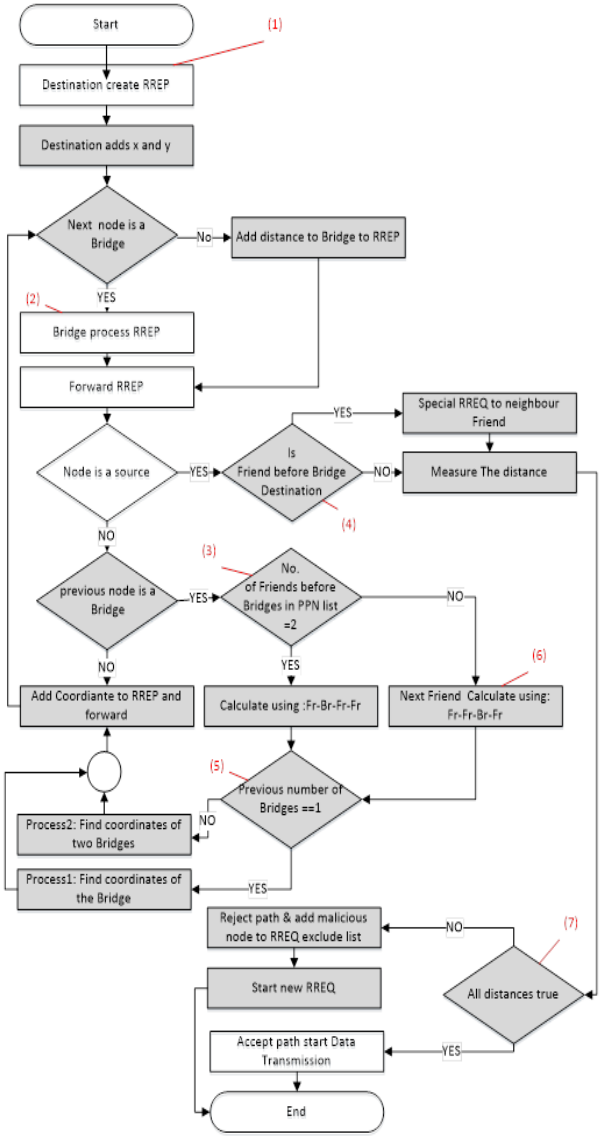

Figure 4: The RREP process for SIMAN and coordinates measurement

3) Wormhole attack detection: The example in Figure 5 demonstrates how the explained technique is used to eliminate different WH types. The network consists of ten Friend nodes, and eight Bridging nodes two of them 7 and 17 are WH nodes. The source node 3

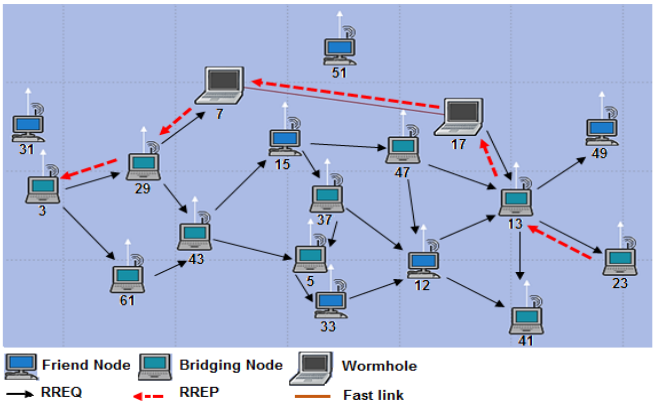

Figure 5: MANET scenario with two WH nodes

wants to send data to destination node 23, and for this purpose, it broadcasts a RREQ message. The two WH nodes make efforts to win the shortest path by processing packets quickly using their Ethernet connection (line connects two black laptops), and the attack comes in three types.

Closed WH attack: Both WH nodes in this attack are invisible/hidden, and any packet passed to them is copied to the output and forwarded to the next node without change. The algorithm detects this attack through the following procedure.

- The initial RREQ process is broadcasted by source node 3 using the AODV routing protocol.
- WH nodes 7 and 17 copy the content of the RREQ message to the output and forward it intact. Therefore, Friend nodes 29 and 13 think they are neighbors.
- Once the destination node 23 receives the RREQ, it creates the RREP message and add its coordinates, then forward the RREP.
- Friend nodes 13 and 29, respectively receive the RREP, and add their coordinates and forward it to the previous node.
- Upon the arrival of the RREP message, the source node measures the distance between nodes and realises the distance between Friend nodes 13 and 29 exceed the threshold, therefore rejects the route.
- Then it creates a new RREQ, and adds the two Friend node addresses to the S-list and sets the S-flag field.
- When both Friend nodes 13 and 29 discover their addresses in the S-list, they reject the RREQ and mark the path between them as invalid since they are not neighbors.

Half open WH attack: In this attack, one of the WH nodes is hidden (node 7), so it does not participate in the routing process, while the other WH (node 17) uses the AODV routing protocol and acts as a normal node. The algorithm detects the attack through the following procedure.

- WH node 7 copies the content of the RREP message received from node 17 to the output and forwards it to Friend node 29.
- Friend node 29 realise that two other Friend nodes 13 and 23 located before the Bridging nodes. Therefore, it uses one-step Bridging node with sequence $(\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3})$ to measure the coordinates.
- Friend 29 is unaware of WH 7 as the latter copies the content of the message to the output, so the hop count remains unchanged.
- Next, source node 3 receives the RREP, measures the distance between nodes inside the path, and discovers the abnormal distance between nodes 29 and 17. Therefore, it rejects the route and starts a new RREQ process by adding the address of 29 and 17 to the S-list.
- The RREQ propagates, and when Friend node 29 detects its address and WH node 17 in the S-list, inside the new RREQ, it drops the RREQ and marks the path with node 17 as invalid.
- In this way, the route that passes through WH node 17 rejected, and the node is eliminated from future routing process.

Open WH attack: When both WH nodes are visible, they act like normal nodes, in terms of processing and forwarding routing packets. The following steps show how the detection procedure is accomplished.

- The WH node 17 forwards the RREP message using the Fast Ethernet link, to WH node 7, which in turn forwards the RREP to the Friend node 29 using its wireless interface.
- When Friend node 29 receives the RREP, it executes the following steps:
  - Find the node addresses in the factor list and discovers that Friend nodes 13 and 23 located before the Bridging nodes, therefore, it executes $(\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3})$ sequence measurement.
  - Compares the number of nodes in the factor list (3 hops) with a hop count (4 hops) and discovers that two Bridging nodes come one after another. Therefore, it uses the two-step measurement.
- When the source node receives the RREP message, it calculates the distance and detects the abnormal distance between WH nodes 7 and 17. Therefore, it rejects the route and starts a new RREQ process with WH nodes in S-list.

4 Algorithm Simulation

In this section, the enhanced algorithm is implemented to MANET nodes using Riverbed (OPNET) simulation software to examine the elimination of the WH and the performance of the network under attack.

The scenario consists of ten Friend nodes with six Bridging nodes (12, 15, 31, 33, 49, 51) and two WH nodes (nodes 7 and 17). Two Friend nodes 3 and 23 have raw data to exchange in both directions, as in Figure 5. Then the scenario is modified to have five different layouts, and nodes are placed randomly at various distances with a fixed data rate of 24Mbps. The full characteristics of the scenarios shown in Table 1.

Several simulations for the scenario are executed to compare the AODV and the enhanced SIMAN algorithm performance under three types of WH node attacks.

Riverbed's IP route report used to collect results that shows the number of hops and its sequence inside the established path. Furthermore, The RDT (Route Discovery Time) and End-to-end-delay for both algorithm simulation measured using various metrics like (Data rate, the distance between two node and topology layouts) to observe the impact of WH elimination on the performance.

Table 1: Simulation scenario parameters

Parameter		Value
Trajectory		Random mobility way-point Movement range: 2000m * 2000m
Distance between two node	- Nodes7 and 17 - Other Nodes	>300m <300m
Data rate	-Nodes7 and 17 - scenario-1 - scenario-2	Outbound (24Mbps), inbound (100-BaseT Ethernet link) 1,2,6,9,12,18,24 and 36 Mbps 24 Mbps
Packet size		512 Byte
Packet reception power threshold		-82.65 dBm
Transmission power		0.005 Watt
Active route time-out		3 sec
Buffer time-out		2 sec
Traffic		500MB, all explicit
Simulation Duration		300 sec

5 Results and Analysis

5.1 Route Discovery Analysis

Simulations were executed for various type of WH attacks for both AODV and SIMAN. The purpose was to examine the successful elimination of WH nodes by the enhanced SIMAN algorithm, through the number and the identity of hops involved in the process as in Figure 6.

Initially, the scenario was simulated without WHs using AODV to compare with results when the WH is introduced. The route report for IP traffic flow (blue dotted arrow) shows a 7 hops path (the nodes 3, 5, 12, 13, 23, 29, 43), and the distance between any two consecutive nodes is (225.4, 238.07, 251.8, 265.6, 272.8, 273.7) meters, respectively.

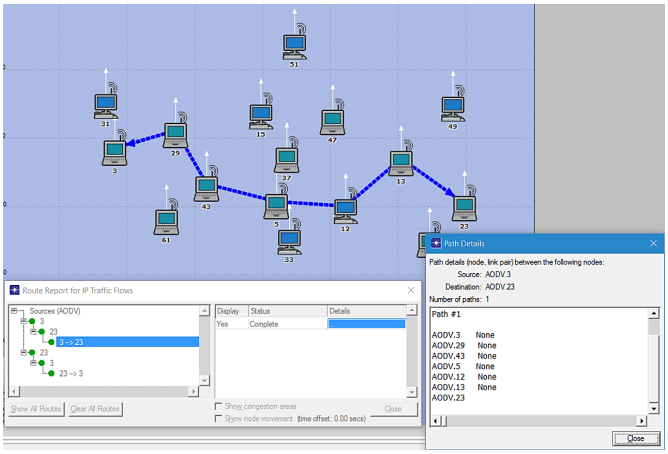

Figure 6: AODV route discovery without WH attack

Open WH attack: The simulation then was repeated for AODV with two visible WH nodes, and the result shows that the WHs managed to divert the route discovery using 6-hop paths (the nodes 3, 7, 13, 17, 23, 29) as illustrated in Figure 7. Using the coordinates values for the nodes inside the path, the distance between neighboring nodes was (238.07, 234.7, 544.1, 253.4, 272.8) meters, respectively.

Using the coordinate values for the nodes inside the path, the distance between neighboring nodes was (234.7, 238.07, 253.4, 272.8, 544.1) meters, respectively. The distance between the two WH nodes, 7 and 17, is 544.1m, which exceeds the maximum threshold distance between wireless nodes [8]. Then, the scenario was simulated again for the SIMAN algorithm, and the result shows that the same original path seen in Figure 6 was established before introducing the WH. Which means the algorithm managed to prevent the two nodes from winning the path, as shown in Figure 8.

Half open WH attack: Afterwards, one of the WHs (node 7) was made hidden to forward the packets

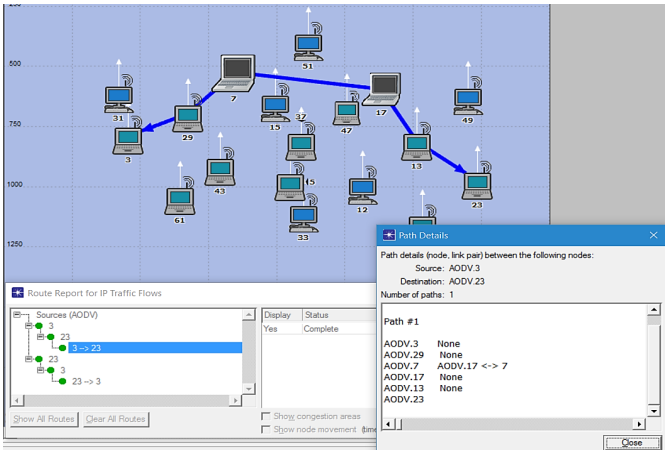

Figure 7: AODV route discovery with open WH attack

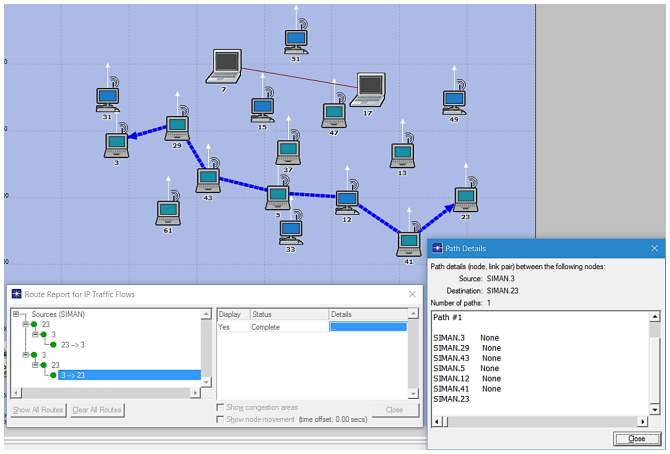

Figure 8: SIMAN route discovery with open WH attack

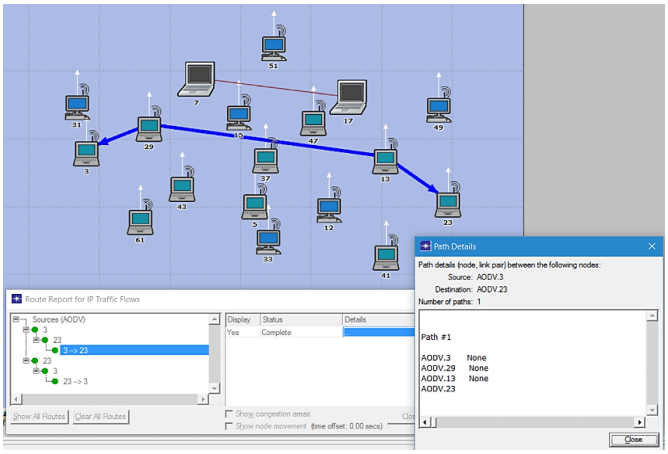

Figure 10: AODV route discovery with closed WH attack

received from Friend node 29 straight to the visible WH node 17 without any change. Then WH node 17 processes the packet using AODV routing protocol. The route report for AODV shows the path consists of 5 hops (nodes 3, 13, 17, 23, 29) as in Figure 9, with distances (238.07, 234.7, 713.7, 253.4, 272.8) meters, respectively. We note that the distance between the Friend node 29 and node 17 is 713.8 meter, which is an indication of hidden WH nodes existence. Subsequently, the same simulation was repeated for SIMAN, in which the outcome was the same as previously established paths seen in Figure 8.

Closed WH attack: In the next simulation, both WH nodes were hidden, so Friend nodes 29 and 13 assumed they are neighbors. The result of the AODV routing protocol shows a path consists of 4 hops (nodes 3, 13, 23, 29) as seen in Figure 10. The distances between these nodes are (238.07, 846.4, 253.4, and 272.8) meters, respectively. We note that the distance between the Friend nodes 29 and 13 exceeds the maximum transmission distance of two nodes (846.4 meters), which indicates the existence of hidden WH nodes inside the path. After that, the simulation was repeated for the SIMAN algorithm, and the result shows that SIMAN managed to eliminate the WH nodes, and used the same route as the previous simulations in Figure 8.

5.2 Route Discovery Time (RDT)

Represents the average round trip time required to receive a RREP message from the destination successfully. The next simulation measured the RDT for both AODV and SIMAN algorithm for various data rates and topology layouts for the three types of WH attacks:

1) Various Data Rates: The RDT results, seen in Figure 11, shows that it took SIMAN 1.28 sec on average more to establish the path in comparison to AODV. Because of the second route discovery process, as the first attempt was rejected because of WH nodes.

   Furthermore, the RDT in both algorithms increased for the open WH attack because the WH nodes need

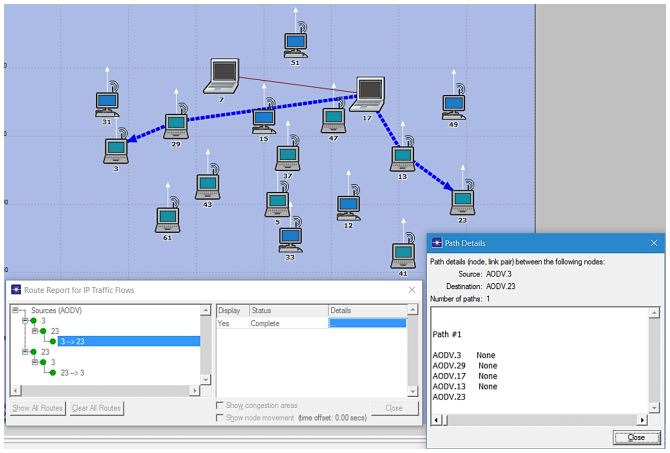

Figure 9: AODV route discovery with half-open WH attack

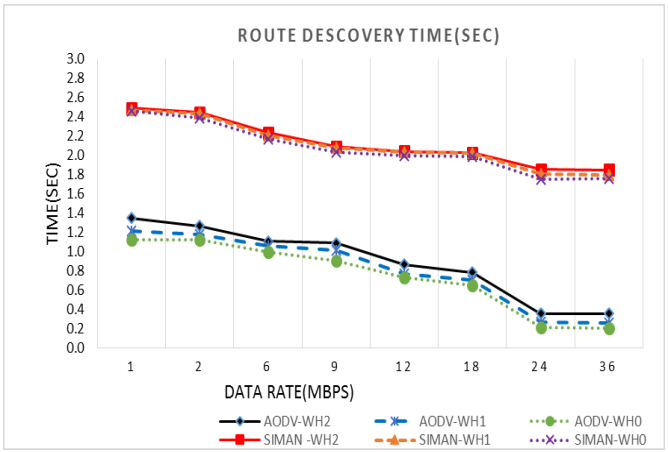

Figure 11: RDT with various data rates

to process packets rather than just forwarding them as in a close attack.

2) Various Topology Layouts: Simulation results for five different topology layouts (with WHs placed randomly in different locations) shows that, when using AODV routing protocol, the WH always divert the path inside the network. While for the SIMAN algorithm, the WH nodes are rejected in all topology layouts as detailed in Table 2.

Table 2: Comparison for number of hops in AODV vs. SIMAN for discovered routes in different layouts

Layout	Traffic 3 ←→ 23			
	AODV		SIMAN	
	Hops	Path	Hops	Path
Layout-1	6	3-43-17-7-51-23	7	3-43-33-5-31-47-23
Layout-2	5	3-17-7-51-23	4	3-5-31-23
Layout-3	4	3-7-17-23	7	3-61-29-5-47-41-23
Layout-4	5	3-43-17-7-23	6	3-12-33-31-23
Layout-5	7	3-5-17-7-12-29-23	8	3-13-43-61-47-49-29-23

Additionally, several different factors influence the RDT in the second scenario, as seen in Figure 12.

- In layout, 1 and 5 an increase of 2.89 sec on average in RDT noticed for SIMAN compared to AODV, due to several route discovery attempts conducted by the algorithm to prevent WH nodes from diverting the path. Likewise, one or more Bridging node coordinate calculation (two for layout-1 and one for layout-5) increases the RDT further.
- Moreover, the RDT in layout-2 took an average 2.46 sec more than AODV, despite having 4 hops inside the discovered route. This result represents a particular case (Sec.4 page 4), in which only two Bridging nodes are in the path. Thus, it requires the source node to send a false RREQ to a neighboring Friend node to get the extra coordinates required for the measurement.
- Finally, the SIMAN algorithm in layout-4 has a greater RDT (2.31 sec) compared to AODV. This is due to three Bridging nodes coordinates calculation that increases the processing time.

5.3 End to End Delay

Simulation result shows that WH attack has an impact on the delay encountered during data transmission. This delay is caused by the speed of processing/forwarding packets by WH nodes inside the selected route. As seen in Figure 13, SIMAN has 0.354 sec on average more delay to AODV, which is due to the number of hops inside the path (AODV-5 hops and SIMAN-6 hops). Because of SIMAN prevention of WH nodes from winning the path. Then the End to end delay was measured for the scenario with different topology layouts, and the result shows variable delay measurements for various topology layouts with an average advantage for AODV 0.248 sec. This advantage is due to different hop numbers inside routes and the WH nodes role in AODV to forward packets faster, as it is illustrated in Figure 14.

6 Conclusion and Future Work

In conclusion, the enhanced algorithm managed to use the existing routing protocol processes to share the node coordinates between nodes inside the discovered path. Which in result it helps toward improving the knowledge of the node's physical location inside the network and enabled the source node to reject routes that have unrealistic distances between two nodes.

Additionally, it prevents malicious attacks without using an extra key-based security solution. The results of distance measurements showed the elimination of several types of WHs introduced by a network scenario. This was observed through the RDT and end-to-end delay, which slightly increased due to SIMANs effort to eliminate and avoid WHs in path discovery. Moreover, several different topologies used with WHs placed in various locations. It was evident from the results that they win the path all the time with AODV routing protocols, while in SIMAN algorithm case simulation reports showed different paths constructed to avoids them.

This algorithm can serve as a platform for further research that can enhance MANET operation through helping the intermediate nodes to repair links by tracking and predict the direction of other nodes movement, which can be a valuable addition to the highly dynamic mobile network. Moreover, sharing other information like nodes remaining battery energy can help the source to select routes that last longer by avoiding nodes with critical battery energy.

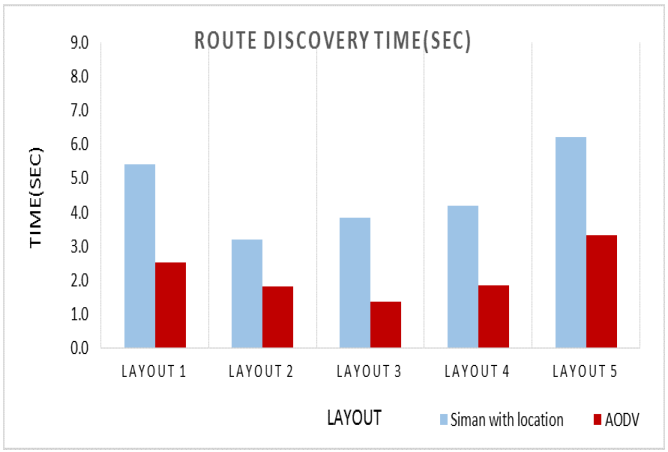

Figure 12: RDT for different topology layouts

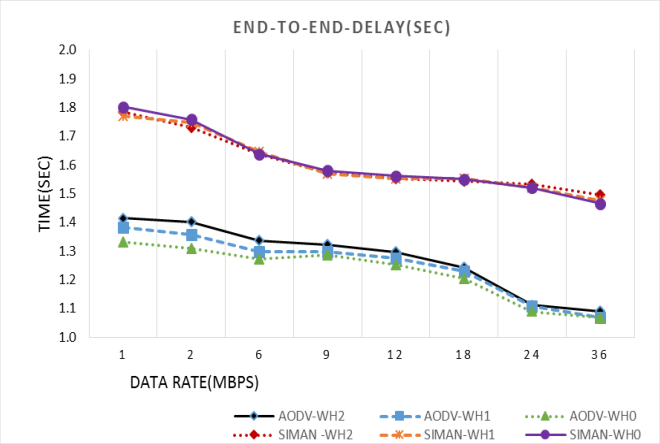

Figure 13: End to end delay for various WH attacks

References

[1] H. Asenov and V. Hnatyshin, "Gps-enhanced aodv routing," in *Proceedings of the International Conference on Wireless Networks (ICWN09)*, pp. 1–7, 2009.

[2] M. Imran, F. A. Khan, T. Jamal and M. H. Durad, "Analysis of detection features for wormhole attacks in manets," *Procedia Computer Science*, vol. 56, pp. 384–390, 2015.

[3] J. Jacob and S. Koyakutty, "An improved flooding scheme for aodv routing protocol in manets," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 3, no. 4, pp. 83–89, 2014.

[4] G. Kadir, T. Kuseler and I. A. Lami, "Smpr: A smartphone based manet using prime numbers to enhance the network-nodes reachability and security of routing protocols," *International Journal of Network Security*, vol. 18, no. 3, pp. 579–589, 2016.

[5] G. Kadir and I. A. Lami, "Siman: A smart identification of manet nodes used by aodv routing algorithm," in *3rd World Congress on Computer Applications and Information Systems (WCCAIS'16)*, pp. 1–7, 2016.

[6] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[7] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[8] Z. Lu and H. Yang, *Unlocking the Power of OPNET Modeler*, Cambridge University Press, 2012.

[9] E. Pagnin, G. Hancke and A. Mitrokotsa, "Using distance-bounding protocols to securely verify the proximity of two-hop neighbors," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1173–1176, 2015.

[10] V. Pierlot and M. V. Droogenbroeck, "A new three object triangulation algorithm for mobile robot positioning," *IEEE Transactions on Robotics*, vol. 30, no. 3, pp. 566–577, 2014.

[11] C. C. Pu, C. H. Pu and H. J. Lee. "Indoor location tracking using received signal strength indicator," in *Emerging Communications for Wireless Sensor Networks*, 2011.

[12] M. Saadoune, A. Hajami and H. Allali, "Distance's quantification algorithm in aodv protocol," *arXiv Preprint arXiv:1411.6320*, 2014.

[13] N. Sahu, D. S. Tomar and N. Pathak, "A modified aodv protocol to detect and prevent the wormhole: A hybrid approach," *International Journal of Computer Science and Network Security*, vol. 15, no. 2, pp. 115, 2015.

[14] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos and J. P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proceedings of the Second ACM Conference on Wireless Network Security*, pp. 193–200, 2009.

[15] A. Shrivastava and R. Dubey, "Wormhole attack in mobile ad-hoc network: A survey," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 293–298, 2015.

[16] B. K. Shrivash and C. Gupta, "A neighbor based efficient worm hole detection and prevention technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, pp. 894–901, 2015.

[17] Y. Wang, C. Westphal and J. J. Garcia-Luna-Aceves, "Using geographical coordinates to attain efficient route signaling in ad hoc networks," in *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'13)*, pp. 1–9, 2013.

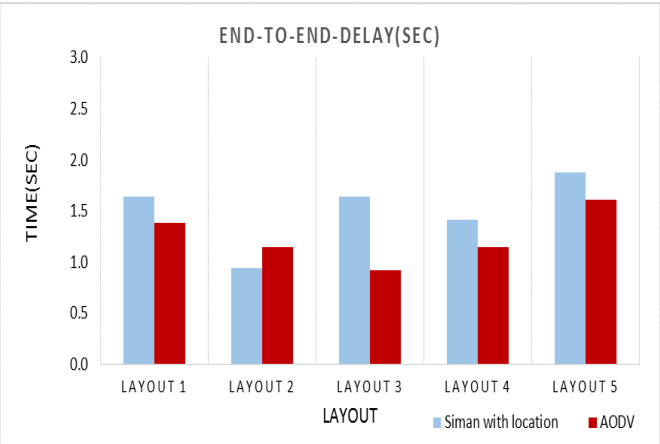

Figure 14: End to End delay for various topology layouts

Biography

Govand Kadir earned his Bachelor of Engineering degree in college of engineering from Baghdad University in 1992. He received his Master of Science degree in in Telecommunication and Computer network engineering in 2006 from London south bank university. In 2017, he completed his Doctoral degree in the Applied Computing Department at The University of Buckingham, UK. Dr. Kadir works since 2007 as a researcher and lecturer for the department of Computer Science and engineering at the University of Kurdistan-Hewler. He is a member of the IT academy sponsored by the council of ministers of Kurdistan regional government of Iraq. Mr Kadir, research focuses on the improvement of routing protocols for Mobile Adhoc Networks and provides protection against malicious devices in these networks.

Ihsan Alshahib Lami is a Reader/Professor in Computer Science at the University of Buckingham, UK. Ihsan worked in Industry for 18 years designing/managing processor and wireless connectivity chips. His current research teams focus on (1) the hybridisation/integration of GNSS and Wireless technologies for optimum localisation and Smart-phone solutions; (2) LTE and Cognitive wireless networks access/security solutions. Please visit http://www.buckingham.ac.uk/directory/dr-ihsan-lami/ for more details.