A Scalable and Secure MANET for an i-Voting System

Kazy Noor E Alam Siddiquee[1], Karl Andersson[2]*, Faria Farjana Khan[1], and Mohammad Shahadat Hossain[3]
[1]*Department of Computer Science and Engineering*
University of Science and Technology Chittagong, Foy's Lake, Chittagong, Bangladesh
{knas11, faria.farjana.khan}@gmail.com
[2]*Pervasive and Mobile Computing Laboratory*
Luleå University of Technology, SE-931 87 Skellefteå, Sweden
karl.andersson@ltu.se
[3]*Department of Computer Science and Engineering*
University of Chittagong, University-4331, Bangladesh
hossain_ms@cu.ac.bd

Abstract

Internet Voting (i-Voting) is an online electronic voting process where a voter can vote staying online from anywhere or connected to a wireless network of a target place. In this paper, a wireless network built with a MANET has been considered for the voting process. National parliamentary voting process of Bangladesh has been taken as the case study. The MANET of the voting process is built using some stationary wireless nodes and mobile wireless nodes. Voters carry mobile wireless nodes using which they can vote. Stationary wireless nodes are installed and deployed in the MANET built in a polling area selected by the National Agency of Election process. These nodes are directly in connection with the national database of voters. Stationary nodes perform the authentication and validation processes of the voter (a mobile node) before the vote is given and casted. The secured transaction of data is the goal to be occurred and routed after a strong authentication and validation of the user has been confirmed. The whole process is completed in a scalable wireless network with a distributed goal based approach. Total processes are followed by secured routing of data in this MANET. The optimal routing protocol among OLSR, AODV, DSR, TORA and GRP has been chosen. Denial of Service (DoS) attacks have been considered as the major threat on nodes in this MANET. The simulation work is done in the OPNET simulator.

Keywords: i-voting; Distributed scalable wireless networks; MANET; Routing protocols; Secure wireless networks.

1 Introduction

Mobile Adhoc NETworks (MANETs) have been one good option for real time applications [1, 2, 3, 4]. Since MANETs are self-configurable and can be organized arbitrarily [5, 6], devices can adopt this topological network easily and free to move around in a certain range of access limit.

This article proposes an application field named as Internet voting (i-voting) system where some wireless nodes (both stationary and mobile) in a MANET are connected taking part in a secure information exchange. MANET is the focused topological framework, which will be configured as single networks in several locations. Each of these MANETs are individually connected with the Internet as shown in Figure 1, where each MANET represents an individual location (see Figure 2).

Each MANET contains three stationary wireless nodes which are connected with coordinating servers

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 8:3 (September, 2017), pp. 1-17

*Corresponding author: Pervasive and Mobile Computing Laboratory Luleå University of Technology SE-931 87 Skellefteå, Sweden, Tel: +46-(0)910-585364 as well as connected with the Internet on behalf of this MANET. The stationary wireless nodes are connected with mobile wireless nodes in the system. The mobile nodes are termed as voters in this i-voting system. Stationary wireless nodes perform authentication and validation of mobile nodes traversing the MANET. At the same time, mobile nodes will connect to secure network for performing secure information transactions. Figure 1 depicts the contextual i-voting system containing several MANETs connected with the Internet. Each MANET is receiving secure information from wireless nodes and sending it to the national database through the Internet.

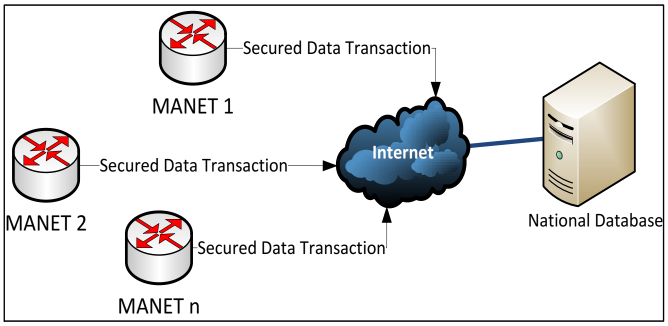

Figure 1: Context network architecture diagram of the system

The number of MANETs connecting to the Internet are *n* for reaching the national database as shown in Figure 1.

The question may arise: Why MANET?

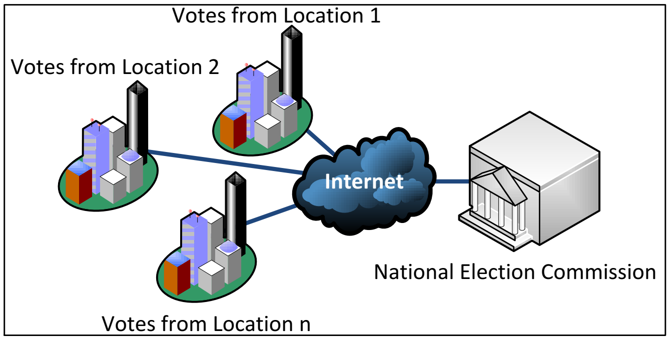

Figure 2: National i-voting system at a glance

The following reasons are considered behind this issue:

1. Each node in a MANET can be a node and a routing hop. The proposed i-voting system requires nodes which will collect data from voters and route it to the destination utilizing routing information which will make the system faster and economic [5, 7].

2. MANETs can perform multi-hop routing when the source and the destination nodes are apart from each other such that they are out of their signal range of access. Hence, there is always a redundant routing available in case of damage of a link or branch [5, 6].

3. MANETs work in a distributed working architecture in terms of security maintenance, routing, caching and node configurations. For this, nodes can assess each other, can retrieve routing or other information from neighbors, can provide security keys such as parameters of hash functions, hashing keys, public or private keys in cryptographic functions and more [5, 6].

4. MANETs support higher node density and mobility of nodes in the network environment. Therefore, the network of a MANET becomes scalable and greater number of users can enter the network for enjoying services [5, 6, 8].

5. Other topologies such as star and mesh are not optimal in large density of nodes, media access and network delays and throughput [9].

The term secure has been used for the reasons mentioned below:

1. Each mobile node (voter) will get connected through a number of authorization and validation confirmed by two nodes.

2. The voting process is a combination of secured processes performed by both a specific stationary wireless node and the voter node.

The MANET is scalable, as in an average case, number of mobile nodes (voters) will grow at a greater number. Density of nodes is not uniform for all MANETs. A single network (MANET) has the following issues:

1. The communication link can be broken any time during a communication session [8, 10, 11].

2. Vulnerabilities of security has been identified which may result loss of data, data stolen or modification of data [12, 13, 14].

3. This network has limited range of wireless signal accessibility [5, 6].

4. Parameters such as throughput, packets loss, delay, network load, energy of nodes, media access have different performance records under different transmission techniques and routing protocols [1, 2, 10, 11].

5. Mobility of nodes has an impact on routing [8, 11].

Design of the network for the i-voting system is projected considering the voting process of a developing country (Bangladesh) where the system is run manually and facing risk factors and challenges [15]. Citizens of the country takes part in this manual voting process to select the candidate of their choice. A greater number of voters [15] participate in this voting system. Since voters need to be present while casting of votes, the MANET is considered to be built in the working place of voting. The proposed i-voting system for the national voting process can be conceptualized from Figure 2. Amount of votes casted from different locations are collected electronically using wireless nodes. Entering of voters in MANETs goes under an authentication and validation process. The voting process is proposed to be secured maintaining security measures. Number of votes casted in a particular location are stored and the information is sent to the national database system.

This article is tackling the following two research questions:

1. What are the security measures for a single MANET of the Internet voting system?

2. How efficiently greater number of users can be handled to ensure optimal routing in the MANET?

Section II highlights the related works, while Section III discusses the methodology used. Section IV presents the results and analysis and Section V concludes the paper.

2 Literature Review

MANETs are widely used in most industrial sectors where faster communication in shorter range network compared to MAN and WAN are being considered [5, 6, 8]. Star and Mesh Topologies were the considering factors for stable network performance and optimal spectrum efficiency [9]. Since MANETs were found to be more efficient in topological performances in a scalable network where substantial growth of nodes is an important factor [8, 16]. As, the Internet voting system has a non-deterministic growth of users (voters) [15], this network needs to be scalable enough to handle such overhead.

Routing in MANETs is a concerning issue and various routing protocols decide routing schemes [1, 2, 3, 8, 17, 18]. For proactive routing, the protocols used are OLSR, GRP, DSDV, WRP, TBRPF and QDRP. Reactive routing schemes use AODV, LMR, TORA, DSR, LQSR protocols. Routing schemes are preferred considering some vital network attributes such as medium access delay, network load, energy of nodes, throughput, packet drops and transmission delay [1, 10, 11, 18]. OLSR, GRP, AODV, TORA and DSR are widely used in industrial and research applications [10, 11] with some selective attributes among these in the network. AODV uses the routing cache and decides upon routes from dedicated entries for each destination in a reactive manner [18]. DSR maintains the routing cache populating multiple entries for destinations whereas TORA functions with the principle of an algorithm named as Link Reversal with a temporary ordered list of entries for destinations. This protocol offers a loop free network with multiple routes to avoid congestion. But it is not capable of using shortest paths for routes [18]. For optimal performances, other algorithms and prediction techniques have been applied [4, 7]. Other researches have chosen Zigbee [11] since it consumes less power, it is simple to deploy and it is cheaper. However, MANETs performed best using AODV and OLSR [1, 10, 18]. The proposed i-voting system will experience a large traffic due to a greater quantity of users in MANETs. Hence, efficient routing scheme is a challenging factor and an optimal routing protocol needs to adopt in the network for the best routing performance considering throughput of traffic, network load, packets dropped, delay and media access delay.

Another challenging issue for individual MANETs is the security. MANETs are vulnerable to major threats and attacks [19]. Compromising of key distributions, privacy of a network user, integrity/authentication data and anti-jamming for denial of service are committed in physical layer [13, 14, 16, 19]. On the other hand, using cryptanalysis compromising of confidentiality, integrity/authentication, digital signature, non-repudiation and access control attacks are performed in upper layers [13, 14, 16, 19]. Repudiation and data corruption occurs in application layer. Session robbing and flooding attacks are done in transport layer. At the network layer, black hole, wormhole, consumption of resources, location disclosing and byzantine attacks are committed whereas traffic analysis and monitoring of disruption at MAC 802.11 occur at data link layer [14, 19]. Previous Internet voting systems experienced substantial attacks [20] and in the paper [20] a threat tree was proposed by Pardue et al. Again, assessing risks in electronic voting system the same author proposed a threat tree for Direct Recording Electronic (DRE) Systems [21]. For the proposed i-voting system, identity management needs to be strong enough for authentication and validation of users in MANETs. Early studies were limited only to decisions based on possible attacks and some of the measurements were taken for attacks at physical layers such as attacks by brute force methods, privacy compromising or attacks on key distribution [13, 16, 20]. However, attacks at upper layers have not been taken into considerations. This article presents the performance of the MANET under an attack done at the network layer which is termed as Black Hole attack [14, 19]. There has been a possible threat from other attacks such Sybil attacks, Wormhole attacks, flooding attacks, Denial of Service (DoS) attacks, overflow of the routing table attacks, and many more [19]. Since multihop links in MANETs make Black Hole attacks more common, it was chosen to observe the performance of the network under that type of threat.

The i-voting system which is the research focus of this article, was not initiated with the term 'Internet' at first. Electronic voting (E-voting) was the first system of automated voting introduced by the Organization for the Advancement of Structured Information Standards (OASIS) in January 2005 and it was implemented in the national election of Estonia [22, 23, 24, 25, 26, 27, 28]. The Zurich government [26, 29, 30] initiated Internet voting and later the Governments of Canada and Switzerland [31, 32] added safety standards in this polling system. Challenges regarding i-voting concept have been pointed out [15, 29, 33] and it came under criticism [34]. Security experts expressed their concerns and yet they could not rely on this system. However, for presidential election in US, Internet voting was adopted in more than 30 states [34]. Major threats have been pointed out and security experts expressed their concerns on protection, electronic ballot, safety of voters, safety of data transactions, confidentiality of votes, accountability, online voting from remote places, accuracy, transparency, and verifiability of elections [15, 34].

Other studies we performed in the area of Wireless Sensor Networks include proposals on systems for efficient flood prediction, smart irrigation, and related areas [35, 36, 37, 38, 39, 40, 1, 41].

3 Methodology

Our proposed system comprises *n* MANETs from *n* locations (as shown in Figures 1 and 2). Each MANET has some stationary nodes named as WN1, WN2 and WN3 as shown in Figures 3 and 4. The mobile node named ”User” in Figures 3 and 4 gets connected in the MANET for voting purpose. Stationary nodes perform the authentication and validation procedure using the security process served by a Security Server. The casting of vote is performed by another stationary node which routes the collected data from user to the Data Server which is connected to the Internet.

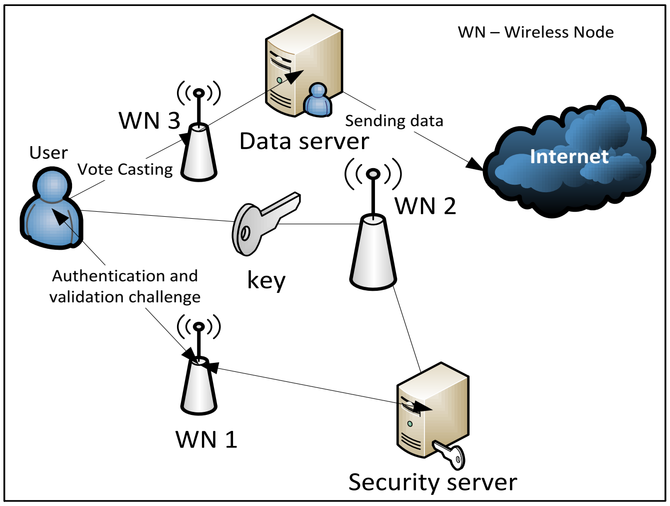

Figure 3: Operation of a single MANET

The voting process can be defined into two phases:

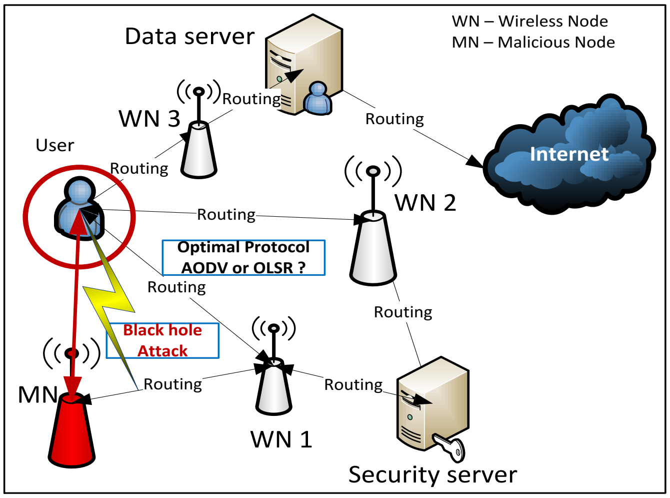

Figure 4: Challenges in MANETs

1. Authentication and validation of a user

A user needs to be authenticated to verify whether s/he is a citizen of Bangladesh using the national voter ID card provided by Peoples Republic of Bangladesh [42]. When a user connects to the MANET at first a wireless nodes receives data of the identity (Biometric data) of the user for verification (Figures 3 and 4). After the authentication purpose has been completed, again the user is assessed whether is the voter of that place [42].

2. Casting of vote

After successful authentication and validation (the voter has not voted redundantly), the voter (the mobile node) receives a key which in turn is used for the encoding purpose of the voting information. The mobile node using the key, sends an encoded message (voting data) to another stationary node which is connected to the Data Server (Figures 3 and 4). This server then send it to the National Database of Election Commission through the Internet (Figures 1 and 2). The total process is figured in the sequence diagram in Figure 5.

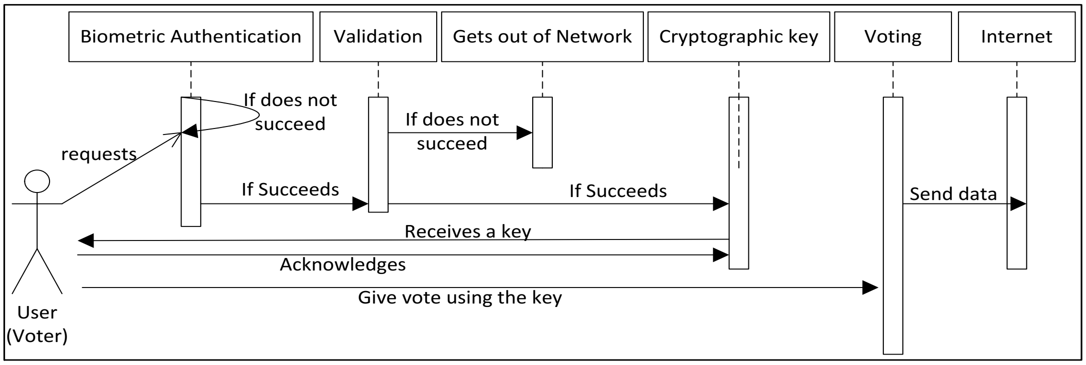

Figure 5: Sequence diagram of voting process of a voter in a MANET

Analysis of Process and Operations

For mathematical analysis, the following attributes are being considered as given in Figures 5 and 6:

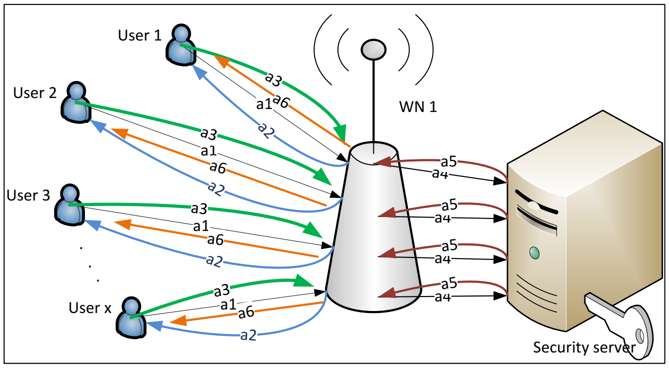

Figure 6: Operational analysis

au = authentication process, wn = wireless node, a = operation, s = Security Server

An authentication process au_1 contains m operations of wn_1, where m contains $m_1 = a_1 + a_2 + a_3 + \ldots + a_m$, where
a_1 is the request from u_1 to connect to wn_1
a_2 is the reply from wireless node wn_1 for biometric authentication to u_1
a_3 is the reply from u_1 with the biometric information to wn_1
a_4 is the biometric data that wn_1 sends to the security server s_1
a_5 happens when wn_1 receives the result from s_1
a_6 happens when wn_1 informs u_1 of the result of authentication

For x users, there will be mx operations for wn_1.

$F(wn_1) = x\sum_{i=0}^{m} a_i$
As $m_1 = a_1 + a_2 + a_3 + \ldots + a_m$ it can be expressed as

$m_1 = \sum_{i=0}^{m} a_i$

Therefore, $F(wn_1) = xm_1 = m_1x$

For best, average and worst cases,

$m_1 = a_1 + a_2 + a_3 + a_4 + a_5 + a_6$

At worst cases, there will be m operations for the total operation of voting. There will not be validation and vote casting operations anymore (from Figure 7). Therefore, only best and average cases are being considered here.

Hence, $mx = O(x)$, which means that our proposed process will take linear time in spite of large quantity of users.

Here, DHCP has been the crucial protocol to handle such large volume of voters.

Again, the wireless node wn_2 will receive a request from wn1 on behalf of u_1 to continue operations for validation of u_1 if the authentication is successful for y users out of x. wn_2 will execute p operations as indicated below:

b_1 = receive request and data from wn_1 for u_1
b_2 = generate query and send to server s_2
b_3 = receives result from s_2
b_4 = inform u_1 on verification result

$m_2 = b_1 + b_2 + b_3 + ... + b_p$ and can be expressed as

$m_2 = \sum_{j=0}^{p} b_j$

For y users, where $y \leq x$

$F(wn_2) = y\sum_{j=0}^{p} b_j$

Therefore, $F(wn_2) = ym_2 = m_2y$

Now at average cases, for y users (out of x) there will be total operations for authentication and validation in wn_1 and wn_2 as shown below:

$F(wn_1, wn_2) = m_1x + m_2y = m_1(y + (x - y)) + m_2y$

$F(wn_1, wn_2) = m_1x + m_2y + m_1(x - y)$, where where $(x - y)$ are those users (voters) who did not succeed in the authentication process.

For best cases (x = y), all x users will get authentication and validation. Therefore, $F(wn_1, wn_2) = x(m_1 + m_2)$
As, both m_1 and m_2 are finite constant numbers, therefore for x or y, either will maintain $O(x)$ or $O(y)$. There will be always a linear time consumed for run time processes in authentication and validation of any quantity of users for Internet voting.

For casting of votes, wn_3 will perform q operations expressed as $m_3 = c_1 + c_2 + c_3 + ... + c_q = \sum_{k=0}^{q} c_k$
If there are z users out of y giving votes, $F(wn_3) = z\sum_{k=0}^{q} c_k$

Therefore, $F(wn_3) = zm_3 = m_3z$

All in all, there will be a total of $F(wn_1, wn_2, wn_3)$ operations from authentication to voting.
$F(wn_1, wn_2, wn_3) = m_1x + m_2y + m_3z = m_1(y + (x - y) + m_2(y + (y - z) + m_3z))$

where $z \leq y \leq z$, $x - y$ users failed to authenticate and $y - z$ users failed in the validation purposes (as sown in Figure 7).

Now, for best cases, where $x = y = z$, $F(wn_1, wn_2, wn_3) = O(n), n = x = y = z$
For average cases, $z \leq y \leq x$ and m_1, m_2 and m_3 being finite and constant numbers of operations, $F(wn_1, wn_2, wn_3) = O(x)$.

Analysis of the network topology and protocols

The MANET contains both stationary and mobile nodes and servers to be connected with Internet as given in figure 3. For routing of data relating to authentication, validation and voting, an optimal routing protocol needs to be chosen. Five different routing protocols have been chosen; OLSR and GRP from the

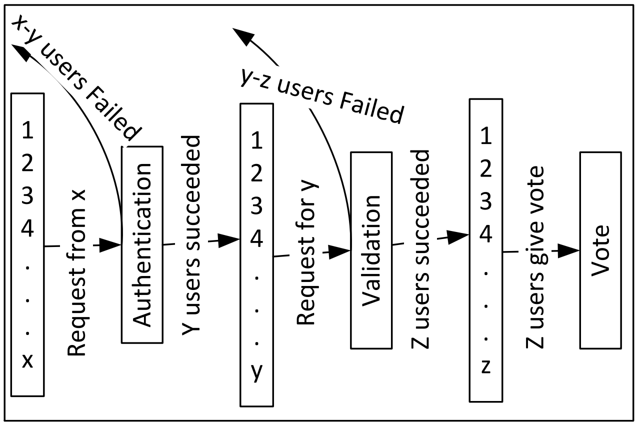

Figure 7: Users in operation

proactive routing protocol suite; and AODV, DSR and TORA from the reactive routing protocol suite.

Under these protocols, the MANET is assessed considering five parameters, namely:

1. Packet Delivery Ratio
2. Media Access Delay
3. Network Load
4. Throughput
5. End-to-End Delay

Primarily AODV and OLSR have been found as the optimal protocols for routing of data in MANETs and finally AODV has been concluded as the best of all.

Analysis of the network security and threats

In MANETs, Black Hole attacks are considered as a network layer threat. Since, AODV and OLSR has been found as the optimal protocols (will be discussed in details in result and analysis section), the attack was simulated on these two protocols only. Figure 4 shows how a malicious node participates in the network and being an active element in the network route, it disrupts the performance of the network. The attack may be occurred either from an internal or external malicious node.

The performance is measured considering end-to-end delay, throughput, network load, and packet delivery ratio for both 16 and 30 nodes. For simulation, end-to-end delay, throughput, and network load are taken as parameters for both AODV and OLSR, whereas packet deliver ratio was chosen only for AODV.

4 Analysis of Results and Discussion

An OPNET-based simulation environment was configured for both 16 and 30 nodes with an area of 100*100 meters. The IPv4 addressing scheme has been adopted with a 600 seconds of simulation duration time. The simulation was performed with five routing protocols considering five distinct parameters.

Table 1: Result of protocols in the MANET

No. of nodes	Metric	AODV	DSR	GRP	OLSR	TORA
16	End-to-End Delay	0.00010	0.00023	0.00011	0.0000691	0.00076
	Media Access Delay	0.00005	0.00008	0.00006	0.0000694	0.00078
	Network Load	1190.326	880.448	1145.192	4102.756	1845.123
	Throughput	8698	4960	8189	33492	2384
	Packets Dropped	2	constant	35	constant	constant
30	End-to-End Delay	0.00044	0.00059	0.00043	0.0000812	0.00079
	Media Access Delay	0.00007	0.00059	0.00019	0.00000067	0.00118
	Network Load	4809.948	2540.236	3184.101	10984.234	5754.972
	Throughput	61793	34988	49124	184895	25187
	Packets Dropped	3	constant	95	constant	constant

4.1 Performance of Protocols in MANETs

End-to-end Delay

Average end-to-end delay = ∑(Time of Destination received packets – Time of Source sent packets)/ Number of packets Using the equation above, for both 16 and 30 node environment, OLSR is found to perform better as can be seen in Table 1. Despite reducing of broadcasts in routes by AODV through maintaining of sequences for each destinations to make AODV faster, OLSR is better for its proactive characteristics.

Media Access Delay

Table 1 shows that OLSR performs better with both 16 and 30 nodes. Every single entry in the routing table for each destination prevents AODV to create loops and instead of that OLSR performs best due to its proactive nature.

Network Load

Table 1 shows that AODV performs well than all other protocols due to reactive routing characteristics. DSR performs better in lower density of nodes whereas for a scalable network AODV has least network load.

Throughput

The proactive nature of OLSR to get better throughput than other protocols in MANETs. But, in higher density of nodes, AODV performs optimally. The measurement is taken using the following equation: Throughput = Size of the Received packet / Time

Packet Dropped

Since, AODV can efficiently utilize resources with less consumption, it has less packet drops compared to other protocols. Delivery of packets can be measured from following equation:

Packet delivery fraction = Number of packets received / Number of packets sent

Since, both AODV and OLSR are dominant in MANETs, they are further assessed in NS3 with attributes of data packets, control packets, overheads and average delay. The result shows that AODV is better than OLSR (from Table 2).

Table 2: Routing overhead of AODV and OLSR in NS3

Protocol	Data Packets	Control Packets	Overheads	Delay (average) in secs
AODV	99	497	83.33	0.0013
OLSR	99	1701	94.50	0.0009

Here, both Table 1 and Table 2 show that OLSR is faster but AODV is found to be more reliable in re-routing of data and adaptable in scalable networks.

Performance of MANETs under malicious attacks

AODV has higher delays than that of OLSR in both 16 and 30 nodes. Under attack, delay rises more sharply in AODV than that of OLSR (see Figures 8 and 9).

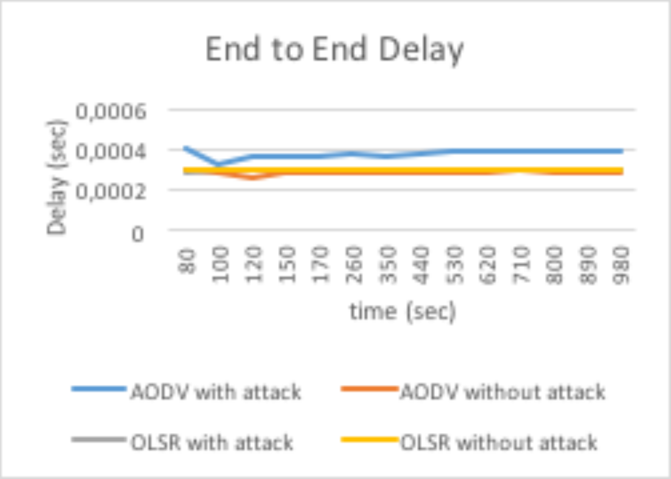

Figure 8: End-to-End Delay for 16 nodes

Throughput of OLSR is greater and under attack, performance of OLSR is affected more in spite of having larger throughput than AODV as can be seen in Figures 10 and 11.

The network load of OLSR is higher compared to that of AODV. AODV is stable more under attack whereas there is a sharp decline of network load in OLSR (from Figures 12 and 13).

Therefore, OLSR is more vulnerable to Black Hole attacks in a network and AODV is more stable. But, OLSR performs better without attack.

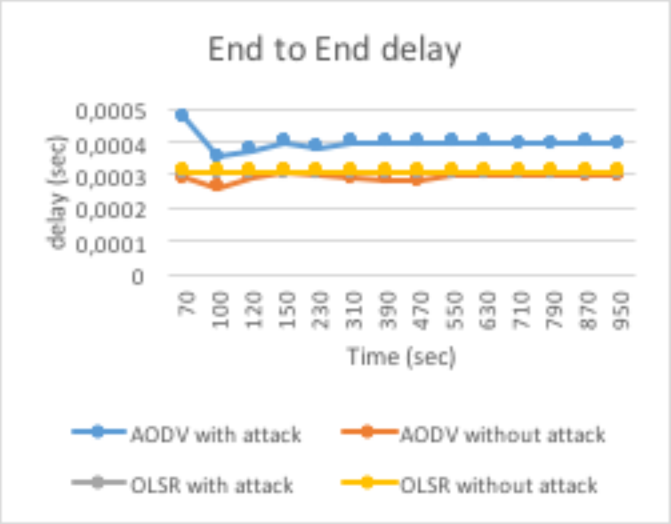

Figure 9: End-to-End Delay for 30 nodes

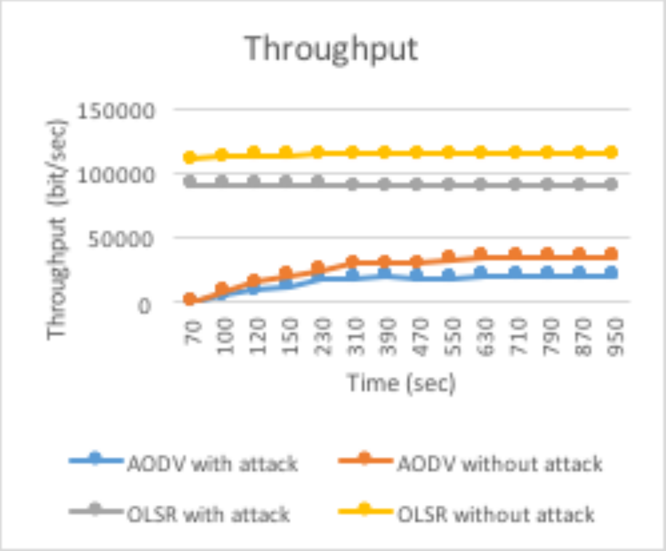

Figure 10: Throughput for 16 nodes

4.2 Results

Packet Delivery Ratio (PDR) is the ratio between packets delivered to the destination end and packets actually sent by the source. The PDR is assessed for AODV under single or multiple attacks in the network. During attacks, the performance of PDR for AODV in MANET falls radically.

5 Conclusion

The proposed Internet voting system comprises several MANETs installed and deployed in different locations of voting area. Despite the concept Internet voting strongly adheres to voting from any location in this globe, the proposed system does not obey. Rather, by building MANETs in different location, voters are invited to visit the location and sign in this network. Staying of voters in different platform

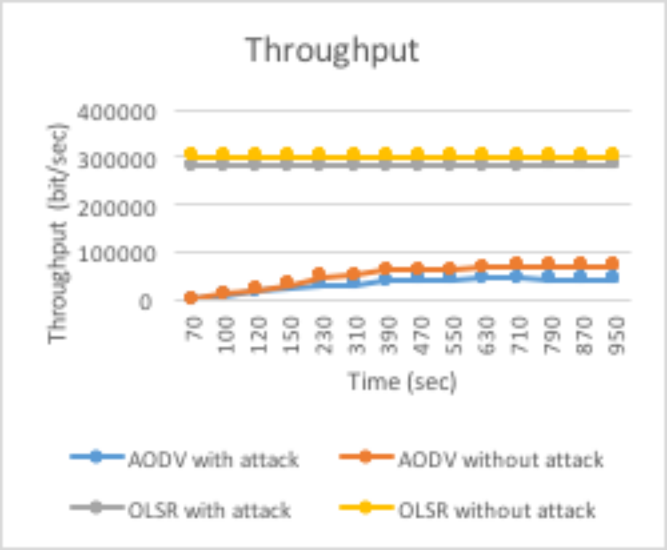

Figure 11: Throughput for 30 nodes

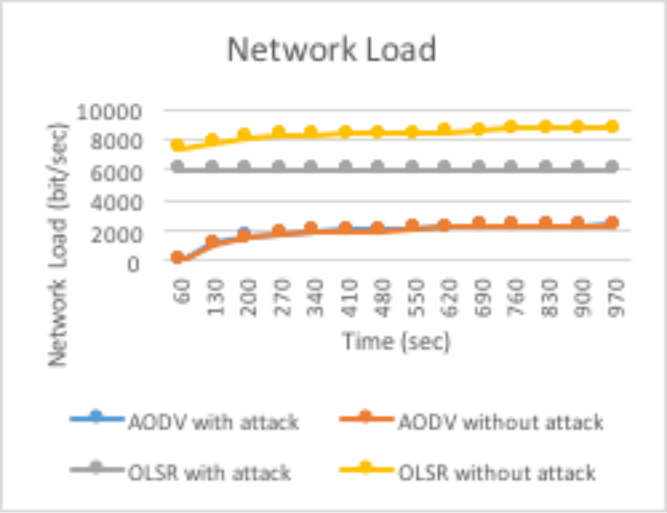

Figure 12: Network Load for 16 nodes

and remote networks increase risks and threats. MANETs perform well in higher density of voters. Growth of the quantity of voters does not affect overall performance and this paper discovered that total operations involved in this system maintain linear time complexity. Therefore, the network is strongly scalable.

Routing of this network is effective under AODV protocol. With the growth of users, performance of MANETs do not degrade in terms of delay, throughput, network load and packets dropped. The network is secured as probable threats at network layer are analyzed. Multi hop links are vulnerable by Black Hole attacks and this paper found that AODV is more stable than OLSR and performs better in spite of higher performances of OLSR in the network.

The i-voting system can effectively and securely route data in the MANET and cast vote. This research has certain limitations on assessment of security issues, since there are other attacks that can occur at the physical, network, transport and application layers. The research was limited only to a

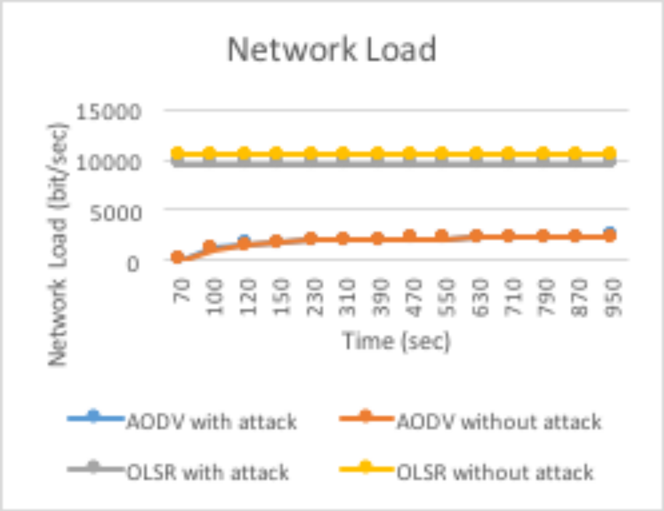

Figure 13: Network Load for 30 nodes

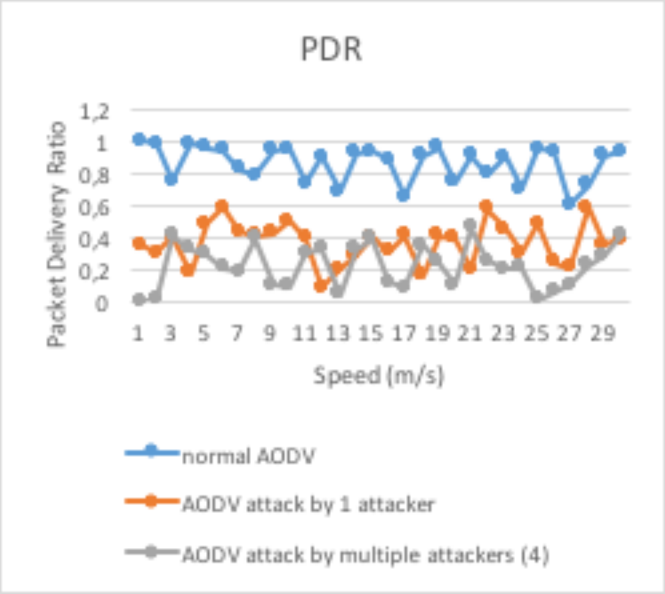

Figure 14: Packet Delivery Ratio for AODV

certain possible types of attacks.

Acknowledgment

This work was supported by Swedish Research Council under grant 2014-4251.

References

[1] K. N. E. A. Siddiquee, K. F. F. Khan, Andersson, and M. S. Hossain, "Optimal dynamic routing protocols for agro-sensor communication in manets," in *Proc. of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC'17), Las Vegas, Nevada, USA*. IEEE, January 2017, pp. 1–5.

[2] F. F. Khan, T. Samira, A. Jana, and K. N. E. A. Siddiquee, "Performance of agro-sensors: Assessment of optimality in routing protocols of manet in wireless sensor networks," in *Proc. of the 2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI'16), Kolkata, India*. IEEE, October 2016, pp. 98–102.

[3] T. Hayes and F. H. Ali, "Location aware sensor routing protocol for mobile wireless sensor networks," *IET Wireless Sensor Systems*, vol. 6, no. 2, pp. 49–57, April 2016.

[4] A. Ali, A. Ikpehai, B. Adebisi, and L. Mihaylova, "Location prediction optimisation in wsns using kriging interpolation," *IET Wireless Sensor Systems*, vol. 6, no. 3, pp. 74–81, July 2016.

[5] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems, 1st Edition*. Prentice Hall PTR, 2002.

[6] C. K. Toh, *Wireless ATM and Ad-Hoc Networks: Protocols and Architectures*. Kluwer Academic Publishers Group, 1997.

[7] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. L. Sun, "Hybrid wireless sensor networks: a reliability, cost and energy-aware approach," *IET Wireless Sensor Systems*, vol. 6, no. 2, pp. 42–48, April 2016.

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, "A scalable and robust communication paradigm for sensor networks," in *Proc. of the ACM International Conference on Mobile Computing and Networking (MobiCom'00), Boston, Massachusetts, USA*. ACM, August 2000, pp. 56–67.

[9] T. Baykas, L. Goratti, T. Rasheed, and S. Kato, "On the spectrum efficiency of mesh and star topology wide area wireless sensor networks," in *Proc. of the 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC'14), Washington D.C., USA*. IEEE, September 2014, pp. 1819–1823.

[10] S. Vanthana and V. S. J. Prakash, "Comparative study of proactive and reactive adhoc routing protocols using ns2," in *Proc. of the 2014 World Congress on Computing and Communication Technologies (WCCCT'14), Trichirappalli, India*. IEEE, February 2014, pp. 275–279.

[11] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2197–2219, April 2016.

[12] E. Atallah and S. Chaumette, "A smart card based distributed identity management infrastructure for mobile ad hoc networks," in *Proc. of the 1st IFIP International Workshop on Information Security Theory and Practices (WISTP'07), Heraklion, Crete, Greece*, ser. Lecture Notes in Computer Science, vol. 4462. Springer, Berlin, Heidelberg, 2007, pp. 1–13.

[13] M. Niedermeier, X. He, H. d. Meer, C. Buschmann, K. Hartmann, B. Langmann, M. Koch, S. Fischer, and D. Pfisterer, "Critical infrastructure surveillance using secure wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 4, no. 4, pp. 336–370, November 2015.

[14] S. Slijepcevic, J. L. Wong, and M. Potkonjak, "Security and privacy protection in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds. CRC Press, 2004.

[15] K. N. E. A. Siddiquee, "The challenges of i-voting and its remedy," in *Proc. of the International Conference on Computational Science and Engineering (ICCSE'16), Beliaghata, Kolkata, India*. CRC Press, October 2016, pp. 183–188.

[16] A. Khosravi and Y. S. Kavian, "Challenging issues of average consensus algorithms in wireless sensor networks," *IET Wireless Sensor Systems*, vol. 6, no. 3, pp. 60–66, July 2016.

[17] V. V. Mandhare and R. C. Thool, "Comparing the performance of proactive and reactive routing protocol in mobile ad-hoc network," in *International Conference on Industrial Instrumentation and Control (ICIC'15), IEEE, Pune, India*. IEEE, May 2015, pp. 394–399.

[18] H. Xu, X. Wu, H. R. Sadjadpour, and J. Garcia-Luna-Aceves, "A unified analysis of routing protocols in manets," *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 911—-922, March 2010.

[19] P. Joshi, "Security issues in routing protocols in manets at network layer," *Procedia Computer Science*, vol. 3, p. 954–960, 2011.

[20] H. Pardue, A. Yasinsac, and J. Landry, "Towards internet voting security: A threat tree for risk assessment," in *Proc. of the 5th International Conference on Risks and Security of Internet and Systems (CRiSIS'10), Montreal, Quebec, Canada*. IEEE, October 2010, pp. 1–7.

[21] H. Pardue, J. P. Landry, and A. Yasinsac, *E-Voting Risk Assessment: A Threat Tree for Direct Recording*

Electronic Systems. Privacy Solutions and Security Frameworks in Information Protection, IGI Global, 2013.

[22] OSCE/ODIHR, "OSCE/ODIHR Election Assessment Mission Report - PARLIAMENTARY ELECTIONS 2006," OSCE/ODIHR, Tech. Rep., 2007.

[23] S. E. O. of Estonia, "General framework of electronic voting and implementation thereof at national elections in estonia," http://vvk.ee/public/EHS/IVXV-UK-1.0-eng.pdf, [Online; Accessed on September 1, 2017].

[24] O. for the Advancement of Structured Information Standards (OASIS), "Election markup language (eml) specification version 7.0," http://docs.oasis-open.org/election/eml/v7.0/eml-v7.0.html, [Online; Accessed on September 1, 2017], 2011.

[25] C. of Europe Committee of Ministers, "Recommendation Record (2004) of the Committee of Ministers to member states on legal, operational and technical standards for e-voting," Council of Europe, Tech. Rep., 2004.

[26] C. of Europe, "Convention for the Protection of Human Rights and Fundamental Freedoms," Council of Europe, Tech. Rep., 1950.

[27] C. of Europe, "Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11," Council of Europe, Tech. Rep., 1952.

[28] A. Prosser and R. Müller, "Electronic voting via the internet," in *Proc. of the 3rd International Conference on Enterprise Information Systems (ICEIS), Setubal, Portugal*, January 2001, pp. 1061–1066.

[29] G. E. G. Beroggi, "Internet voting: An empirical evaluation," *Computer*, vol. 47, no. 4, pp. 44–50, June 2014.

[30] C. of Europe, "E-voting," http://www.coe.int/en/web/electoral-assistance/e-voting, [Online; Accessed on September 1, 2017].

[31] N. J. Goodman and J. H. Pammett, "The patchwork of internet voting in canada," in *Proc. of the 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE'14), Lochau, Austria*. IEEE, October 2014, pp. 1–6.

[32] J. H. P. N. Goodman and J. DeBardeleben, "A Comparative Assessment of Electronic Voting: Prepared for Elections Canada by Canada-Europe Transatlantic Dialogue," Carleton University, Tech. Rep., 2010.

[33] K. Butterfield and X. Zou, "Analysis and implementation of internet based remote voting," in *Proc. of the 11th International Conference on Mobile Ad Hoc and Sensor Systems (MASS'14), Philadelphia, Pennsylvania, USA*. IEEE, October 2014, pp. 714–719.

[34] S. Horwitz, "More than 30 states offer online voting, but experts warn it isn't secure," https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/?utm_term=.2b0f4e403ef3, [Online; Accessed on September 1, 2017], 2016.

[35] K. Andersson and M. S. Hossain, "Heterogeneous wireless sensor networks for flood prediction decision support systems," in *Proc. of the 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'15), Hong Kong, China*. IEEE, April 2015, pp. 133–137.

[36] S. Thombre, R. U. Islam, K. Andersson, and M. S. Hossain, "Performance analysis of an ip based protocol stack for wsns," in *Proc. of the 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'16), San Francisco, California, USA*. IEEE, April 2016, pp. 360–365.

[37] K. Andersson and M. S. Hossain, "Smart risk assessment systems using belief-rule-based dss and wsn technologies," in *Proc. of the 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE'14), Aalborg, Denmark*. IEEE, May 2014, pp. 1–5.

[38] S. Thombre, R. U. Islam, K. Andersson, and M. S. Hossain, "Ip based wireless sensor networks: Performance analysis using simulations and experiments," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, no. 3, pp. 53–76, September 2016.

[39] R. U. Islam, K. Andersson, and M. S. Hossain, "Heterogeneous wireless sensor networks using coap and sms to predict natural disasters," in *Proc. of the 8th IEEE International Workshop on Mobility Management in the Networks of the Future World (MobiWorld'17), Atlanta, Georgia, USA*. IEEE, April 2017.

[40] Z. Abedin, A. S. Chowdhury, M. S. Hossain, K. Andersson, and R. Karim, "An interoperable ip based wsn for smart irrigation systems," in *Proc. of the 14th IEEE Annual Consumer Communications & Networking*

Conference (CCNC'17), Las Vegas, Nevada, USA. IEEE, January 2017, pp. 1–5.

[41] Z. Abedin, S. Paul, S. Akhter, K. N. A. Siddiquee, M. S. Hossain, and K. Andersson, "Selection of energy efficient routing protocol for irrigation enabled by wireless sensor networks," in *Proc. of the 42nd IEEE Conference on Local Computer Networks Workshops, Singapore*. IEEE, October 2017.

[42] E. C. of Bangladesh, http://www.ecs.gov.bd, [Online; Accessed on September 1, 2017].

Author Biography

Kazy Noor E Alam Siddiquee is based in Chittagong, Bangladesh and serving as an Assistant Professor in the Department of Computer Science and Engineering at the University of Science and Technology Chittagong. His research field surrounds computer visions and wireless ad-hoc networks. He has applied computational intelligences in e-Governance, Surveillance & security and Food Bank in perspective in light of current real time problems in third world countries such as Bangladesh.

Karl Andersson (Senior Member of IEEE) has a M.Sc. degree in Computer Science and Technology from Royal Institute of Technology, Stockholm, Sweden and a Ph.D. degree in Mobile Systems from at Luleå University of Technology, Sweden. After being a postdoctoral research fellow at the Internet Real-time Laboratory at Columbia University, New York, USA and a JSPS Fellow with National Institute of Information and Communications Technology, Tokyo, Japan, he is now Associate Professor of Pervasive and Mobile Computing at Luleå University of Technology, Sweden. His research interests include Mobile Computing, the Internet of Things, Cloud Technologies, and Information Security.

Faria Farjana Khan graduated from the Department of Computer Science and Engineering of University of Science and Technology Chittagong. Her research interests span Wireless Ad-hoc networks.

Mohammad Shahadat Hossain is a Professor of Computer Science and Engineering at the Chittagong University (CU), Bangladesh. He did both his MPhil and PhD in Computation from the University of Manchester Institute of Science and Technology (UMIST), UK in 1999 and 2002 respectively. His current research areas include e-government, the modeling of risks and uncertainties using evolutionary computing techniques. Investigation of pragmatic software development tools and methods, for information systems in general and for expert systems in particular are also his areas of research.