A Trust Enhanced Routing Model for Secured Ad Hoc On-demand Distance Routing Vector

Santosh Raj Timilsena[1]*, Arun K. Timalsina[2]

[1] *Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus, Pulchowk, Lalitpur*
***Corresponding author**: timilsena.santoshraj@gmail.com

Abstract

Mobile ad hoc networks (MANETs) represent complex distributed systems that form stand-alone groups of wireless terminals. Although the principle of wireless, structure-less and dynamic networks is attractive, there are still some major security flaws that prevent commercial expansion. Most of the solutions proposed are based on cryptographic implementations which are immune only to specific type of threats and introduces significant routing overheads. Introducing a trust management procedure in a protocol that provides encryption procedures to authenticate messages and hash functions to protect mutable fields increases the capability of the network to address security threats. This paper presents a modified approach for Ad-hoc On-demand Distance Vector (AODV) protocol to implement trust model together with cryptographic features. A proactive table driven approach is proposed to create a trust table in each node and routing packet flow is restricted only to nodes with certain trust values which enhances routing efficiency. Inclusion of trust model aims to identify the misbehaving nodes based on their behaviours and isolate them from the network. This mechanism offers more resilience to attack from malicious nodes, while also promotes collaboration among cooperative nodes and penalizes selfish nodes.

Keywords

MANET – AODV – Cryptography – Trust

1. Introduction

An ad hoc network is a network without any infrastructures. The network is created in ad hoc fashion by the participating nodes without any central administration. There are no dedicated routers or network management nodes, but the participating nodes work in peer-to-peer fashion and act as both servers and routers. The nodes are usually assumed to be independent and do not need to have any kind of affiliation from before, so both computational resources and link capacity might vary greatly from node to node. Nodes are not assumed to be static, but are allowed to move freely inside a network, as well as leave or enter the network at any time. As in a general networking environment, mobile ad hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is obvious that most security threats target routing protocols which is the weakest point of the mobile ad hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols. However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically a "secure" protocol is only good at protecting the network against one specific type of attacks. Protocols for secure routing usually apply cryptography and thus come with a significant increase in complexity and computational overhead. In order to achieve security requirements, complicated encryption techniques and additional information in the routing packets are used which reduces overall routing efficiency. This paper is based on AODV. AODV is a dynamic reactive routing protocol designed for larger ad hoc networks. AODV routing protocol is a pure on-demand route acquisition system. Nodes that are not a part of active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Moreover, a node does not have to discover and maintain a route to another node until the two needs to communicate, unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes. When the local connectivity of the mobile node is of interest, each mobile node becomes aware of the other nodes in its neighbourhood by the use of several techniques, including local broadcasts known as hello messages. The routing tables of the nodes within the neighbourhood are organized to optimize response time to local movements and provide quick response time for requests for establishment for new routes. Within the limits imposed by worst-case route establishment latency as determined by the network diameter, AODV is an excellent choice for ad-hoc network establishment. It is useful in applications for emergency services, conferencing, battlefield communications, and community-based networking. AODV reduces memory requirements and needless duplications. It also has quick response to link breakage in active routes. The most important feature it has is loop-free routes maintained by use of destination sequence numbers and most important scalable to large populations of nodes. AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. Some of the common attacking techniques include cache poisoning, fabricating or forging the route messages, creating a wormhole, spoofing, packet dropping (black hole), malicious flooding(Denial of Service), rushing attacks, where the malicious or compromised nodes quickly disperse wrong routing messages to block legitimate messages from getting accepted [1]. These attacks may result in routing loops, network partitions, sleep deprivation (exhausting the battery) etc. While the on-demand property of AODV results in low protocol overhead and adaptability to host movement, it makes the protocol vulnerable to real time attacks on different nodes at different points in time. Since the routing functions and messages are distributed, it is difficult to trace back the sources of false information.

2. Related Work

To secure information many different approaches have been proposed over the years. The most common approaches use the DES and the RSA Cryptosystem [2]. A secure version of AODV called SAODV [2, 1] provides features such as integrity, authentication and non-repudiation of routing data. The SAODV addresses the problem of securing a MANET network. Two mechanisms are used to secure the message. Digital Signature is used to authenticate and preserve integrity of non-mutable field data in routing packets. For non-mutable field the authentication is done in an end-to-end manner. Hash chain is used to secure mutable field like hop count information. SAODV is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation [1].

A trust management scheme helps to build safer paths. Trust could be described as the probability wherewith an agent will perform an action, before this action could be detected. The trust value of an agent could be defined through interactions and opinions of the other agents regarding an action of the agent. Different trust models are described in [3, 4, 5] for wireless networks. Actual implementation of these trust models in MANETs are described in [6, 7]. A novel way of implementing trust in MANET in energy constrained environment is proposed in [8]. In previous works [9, 10], the SAODV protocol was extended by applying trust model to promote the collaboration of the cooperating nodes, penalizing the selfishness. Trust management scheme along with cryptography makes routing protocol more robust [9]. A trust table is introduced in network where each node is assigned with a trust values. The approach proposed in [10] manages the trust between nodes and also addresses the energy efficiency of nodes.

In this paper, we apply the trust model into SAODV. Our paper work presents a scheme for trust implementation to optimize use of network resources. Features of both proactive and reactive routing of MANETS are incorporated to propose M-TAODV (Modified trusted AODV).

3. Proposed Trust Management Scheme

The new protocol, called M-TAODV (Modified Trusted AODV), overlays the trust model proposed in [8] over SAODV with modifications in routing procedures of AODV to address routing efficiency. The proposed routing approach is described using trust based approach and cryptographic approach. The proposed routing scheme assumes a self organized network for trust implementation. Involvement of trust third party is assumed for implementation of cryptographic features.

The concept of trust used is a combination of friendship and interaction. The trust value of any node is determined from ones perspective about the node, recommendations from other nodes and its history of interactions. The trust value of a node gradually decreases if a node starts misbehaving. The communications through the node is restricted if trust value goes below predefined threshold.

3.1 Trust based approach

Trust is measure of uncertainty with its value represented by entropy. Information Theory states that entropy is a nature measure for uncertainty. Entropy based trust values [4] is defined as:

$$T\{\text{Subject: agent, action}\} = \begin{cases} 1 - H(p) & \text{for} \quad 0.5 < p < 1 \\ H(p) - 1 & \text{for} \quad 0 < p < 0.5 \end{cases} \tag{1}$$

Subject TSubject : agent, action denotes the trust value of the relationship subject : agent, action, Psubject : agent, action denotes probability that the agent will perform the action in the subject's point of view and probability is opinion of subject only. Function H(p) denotes the entropy of a variable p. The entropy function is given by equation (2).

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{2}$$

Trust value is a continuous real number lies in interval $[-1,1]$. Trust value is negative for $0 < p < 0.5$ and positive for $0.5 < p \leq 1$. The trust management architecture used in our system model depicted in Figure 1 has been derived from [8].

In the architecture shown in Figure 1, the history of interactions module is created to store records on interactions between nodes in a suitable data structure. The history of interactions a node A with another node B, recorded at A is denoted as $H_A(B)$. In list $H_A(B) = \{H_1, H_2, \ldots, H_i, \ldots, H_n\}$, kept at node A, each entry H_i represents the trust record of a single interaction with node B. H_i is defined by the triple $H_i =< e_i, s_i, t_i >$, where e_i is the evaluation of the interaction, s_i is the type of interaction provided and ti is the time the interaction had happened. During direct or indirect computation, this module is maintained and updated by the history maintenance module.

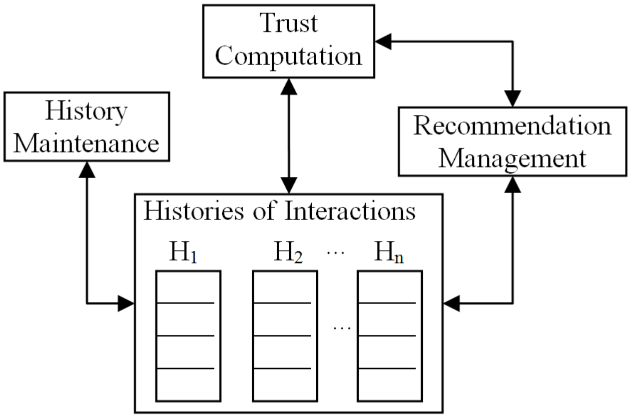

Figure 1: Probabilistic Trust Management Architecture

3.1.1 Trust Computation

Trust computation module depicted Figure 1 is responsible for trust computation. When a node joins a network and prior to each interaction occurring between nodes, trust values must be calculated. The trust values can be calculated using either recommended trust computation or direct trust computation. At the initial stage of network setup or when a node first joins a network recommendation trust computation is performed. Direct trust computation is used to compute trust values of nodes when they interact with each other during communication.

Prior to running the indirect trust computation, more information is required such as the recommendations obtained from recommender nodes and the trustworthiness of these nodes. Trust recommendation request (TRREQ) packets are sent by nodes wishing to know recommendation of other nodes. Judgments on recommenders and their recommendations are made based on trust recommendation reply (TRREP).

Let a node A wishes to know about the trustworthiness of node B. It sends TRREQ to node C and gets a TRREP. Then, trust value of B recorded in A is given by the product of trust value of B with respect to C and its trustworthiness:

$$T_A(B) = T_A(C).T_C(B) \tag{3}$$

When nodes start to communicate, they interact with each other. Based on the history of interactions, direct trust value is computed after each interaction. Trust value of node B for node A is computed by node A using direct trust computation as:

$$T_A(B) = (p_s + 1)/(p_s + p_f + 2) \tag{4}$$

Where p_s and p_f are weighted value of successful and failure interaction given by

$$p_s = \sum_{i=1}^{n} w^{t_c - t_i} \tag{5}$$

$$p_f = \sum_{i=1}^{m} w^{t_c - t_i} \tag{6}$$

Where n is number of successful interactions and m is number of failure interactions. The parameter w is weight used to account trust values with respective to time and t_c and t_i represent current time and initial time respectively.

3.1.2 Trust update

The nodes need to store the trust values about the other nodes. Concurrently with the routing table, a trust table is introduced. The table is updated periodically, so the recommendations and the direct observations are stored in buffers until the update. If T_{i-1} is a trust record in table and T_{cal} be its calculated trust value based on recommended trust computation or direct trust computation, then the updated trust value Ti is given by:

$$(1 - T_i) = a(1 - T_{i-1}) + b(1 - T_{\mathrm{cal}} - d) \tag{7}$$

where a and b are weighting factors and d is correction factor.

3.2 Cryptographic approach

Cryptographic features are added to AODV in this case is similar to SAODV. It is assumed that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme. Two mechanisms are used to secure the message. Digital Signature [10] is used to authenticate and preserve integrity of non-mutable fields' data in route request and route reply messages. For non-mutable field, the authentication is done in an end-to-end manner. Hash chain [7] is used to secure mutable field like hop count information. The primary security requirement that SAODV satisfies is the import authorization, which is the authorization to update routing information only when the information is received by the destination itself. It needs other security services, such as integrity and source authentication. Integrity ensures that the message information was not modified by intermediate nodes, whilst source authentication is needed to verify that the node is who claims to be. These properties combined define data authentication, and they are obtained with digital signatures and message authentication techniques.

3.2.1 Digital signature

To protect the field integrity, SAODV protocol uses the digital signatures to secure the packet. In this way, the fields cannot be modified by any node except the one that generates the packet. The only field not involved in this process is the hop count field, because each node that retransmits the packet needs to increase the value in the field. To address the issue of allowing the intermediate nodes to reply to route requests if they have an active path to the destination, the protocol takes in account two possibilities. In the first, each intermediate node will not reply to the request also if it has a route to destination. The second one allows the reply by other nodes, which need to include the original signature of the destination (stored in a cache), signing the fields modified by them. These two approaches are called respectively Single Signature Extension and Double Signature Extension. Packets generated using these extensions allow each node to verify the validity of messages. If the verification fails, the node discards the information in the packet.

3.2.2 Hash Chain

The hop count field has to be modified by each node that forwards the RREQ or RREP packet. The hash chain mechanism helps any intermediate node to verify that the hop count has not been altered by any malicious node. A hash chain is formed by applying a one way hash function repeatedly to a seed (random number). Every time a node originates a RREQ or RREP message, it put a random number (seed) in the "hash" field, and the TTL in the "max hop count" field. The "top hash" field is filled by applying "max hop count" times the hash function h to the value in the "hash" field.

$$\text{TOP\_HASH} = h^{\text{MAX\_HOP\_COUNT}}(\text{seed}) \quad (8)$$

Where, h is a hash function and $h^i(x)$ is the result of applying the function $h(x)$ to the power i times.

To verify the hop count, intermediate nodes regenerate the TOP_HASH using equation (9).

$$\text{TOP\_HASH} = h^n(\text{Hash}) \quad (9)$$

Where n = (Max_Hop_Count – Hop_Count) If the result of this operation is equal to the information contained in the "top hash" field, the information is verified. Before rebroadcasting, the node hashes the value in the Hash field to account for the increment in the hop count.

3.3 Routing Approach

Different approach is used for routing than in original AODV. The approach is divided into two phases. In first phase a proactive method is applied where the trusted nodes and routes are identified using trust model while in second phase routes to desired communicating nodes are identified using cryptographic approach similar to that in SAODV.

Proactive phase occurs at the time of network setup or each time a node joins the network. In this phase a trust table is created using trust model described above. Here, each node assigns trust values of other nodes in its trust table based on its knowledge about them. For complete trust value 1 is assigned and -1 is assigned for a complete distrust. The node assigns trust value 0 if it is uncertain about their trustworthiness and initiates a recommended trust request procedure. Two new packet typologies are introduced allowing the nodes to send and receive recommendations: Trust Recommendation Request (TRREQ) and Trust Recommendation Reply (TRREP). TRREQ contains the request originator and a list of the requests about the agents of which the originator needs to know if they are reliable or not. TRREP contains the request originator, the recommender, who generates the reply, and a list of couples <*agent, trust value*>. To secure those packets, a signature extension is added to the packets, in a similar way in which other SAODV packets are secured. If node A obtains k numbers of recommendation about B, the equation (3) can be rewritten for every $T_A(i) > 0$ to obtain its trust value as:

$$T_A(B) = (\sum_{i=1}^{k} T_A(i).T_i(B))/k \quad (10)$$

Using this trust value, the trust value in table is updated using equation (7). Ignoring value of d in equation (7), it can be simplified as:

$$T_i = 1 - a(1 - T_{i-1}) - b(1 - T_{\text{cal}}) \quad (11)$$

The obtained value is normalized to the range [-1, 1] before update. This process also lists the available trusted paths to the trusted nodes. The process is repeated in periodic fashion to update trust values and routes.

The other phase of trust management occurs during reactive phase which is imitated when a node needs to communicate with other. Let a source node S needs to communicate with destination node D, S first checks its routing table for any available trusted route. If there is one it forwards the route request packet using this same route to check its cryptographic verification. In case no trusted routes are available in cache, route request is sent to the neighbours with positive trust values. The intermediate nodes also check if trusted routes to destination are available, before forwarding to its trusted neighbours for route discovery. In each hop of packet transmission cryptographic verification is performed in same manner as in SAODV. When route request packet arrives to the destination it generates route reply and forwards back to source using reverse path that was setup during transmission of route request.

If route was not available only using nodes with positive trust values, S broadcasts the route request packet to all neighbors and the same process of route discovery is repeated.

Destination node is responsible for route selection form route discovery if multiple routes are available. Route selection is based route trust (RT) which depends on average trustworthiness of nodes and hop count. For a route with n number of nodes and x hop count

$$\text{RT} = a(\text{max\_ hop\_ count} - x) + b(\sum T/n) \quad (12)$$

Where a and b are weight given to minimum hop count and maximum average trust of nodes.

After each interaction each node calculates the trust value of its interacting nodes using direct trust computation. For N number of interactions direct trust equation can be rewritten using equations (5) and (6) in equation (4) as:

$$T_A(B) = (1+\sum_{i=1}^{N} w^{t_c-t_i}K_i)/(1+\sum_{i=1}^{N} w^{t_c-t_i}P_i) \quad (13)$$

In this equation Ki=0 for failure interaction and 1 for successful interactions while Pi = 1 for each interactions. The trust values in the table are again updated using equation (11) after normalization.

4. Metrics for evaluation

In MANET there are several factors which characterize the network performance making all those metrics highly dependent on each other. Packet delivery ratio (PDF) is the ratio of successfully delivered packets at the destination to the number of generated packets. It shows the capacity of each protocol for successful transmission of data packets to the destination, the reliability of the routing protocol. This metric is a measure for the reliability and correctness of routing protocol.

Normalized routing load (NRL) is the total number of routed packets transmitted per data packet delivered at the destination. It allows analyzing other metrics pointing to the routing load.

Average end to end delay (AED) measures the time that packets travel from the source to the application layer at the destination node.

5. Simulation Analysis

The results of this paper are based on extensive simulation of different network environments in determining the performance and security issues of AODV routing protocol and its security extensions. Protocol efficiency was analyzed in different environment using various attributes. The detailed analysis of AODV, secured extensions of AODV (SAODV) and proposed trusted version of AODV (M-TAODV) were performed. The parameters used to obtain the results are shown in the Table 1.

Table 1: Simulation scenario

Parameter	Value
Simulator	NS-2
Mobility Model	Random Waypoint Model
Simulation Time	500 seconds
No. of Nodes	10 to 100
No. of Malicious Nodes	20% of Nodes
Simulation Area	500m × 500 m
Node Velocity	0 to 25 m/s
Pause Time	0 to 100 seconds
Traffic Type	CBR
Packet Size	512 Bytes

With AODV, when the number of malicious nodes was increased, the number of data packets dropped by them also increased. This was the cause for the decline in the PDF metric of AODV. SAODV was found to be vulnerable to impersonation attacks though it was found to be immune to attacks like route modification, hop count modification and route drop attacks. The PDF metric of M-TAODV remained unchanged even when number nodes are increased as shown in Figure 2.

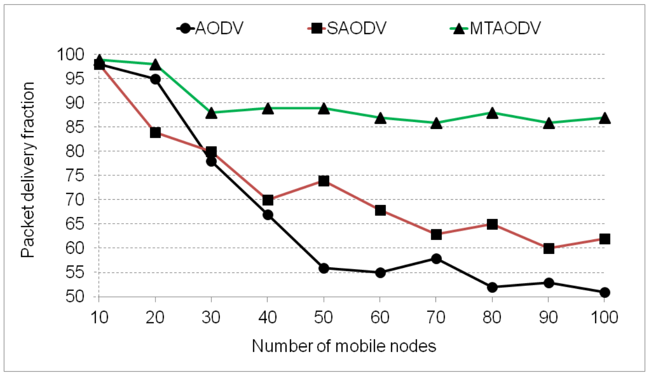

Figure 2: Effect on packet delivery fraction

The AODV protocol was also fooled by the packet modification attack and impersonates attack. There were no new routing packets generated, so the number of routing packets was nearly constant. The NRL metric is inversely proportional to the number of received data packets. Consequently, the NRL metric was slightly raised when the number of malicious nodes was increased increases. But, with SAODV, during route modification attack, due to its capability of detecting and discarding changed routing packets, many more new routing packets were sent to find a new route. This reason caused the increase in the NRL metric of SAODV. In case of M-TAODV the routing packets from the only trusted nodes were routed which significantly decreased the number of routing packets causing significant improvement in NRL metrics as shown in Figure 3.

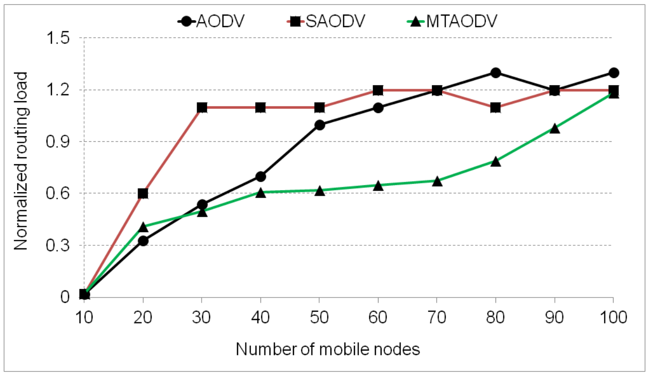

Figure 3: Effect in normalized routing load

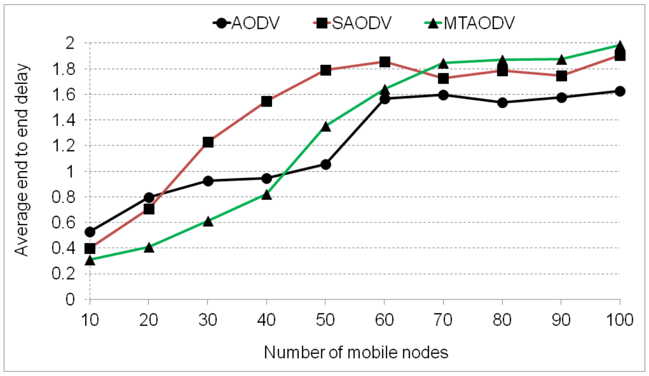

Figure 4: Effect on average end to end delay

Performance of AODV was found better in terms of AED even in malicious scenario as shown in Figure 4. The reason of higher value of AED in SAODV was due to the processing time involved in trust verification and cryptographic processes involved. AED metrics of M-TAODV though better for lower number of nodes; it degrades with the number of nodes as the probability of taking longer routes with higher trust values increases.

Route selection time for M-TAODV is lower as shown in Figure 5. Maintenance of cache for trusted routes in network in each node is the reason for this improvement. For higher values of nodes, possibility of available trusted route to destination decreases and there is rapid increase in route selection time of M-TAODV.

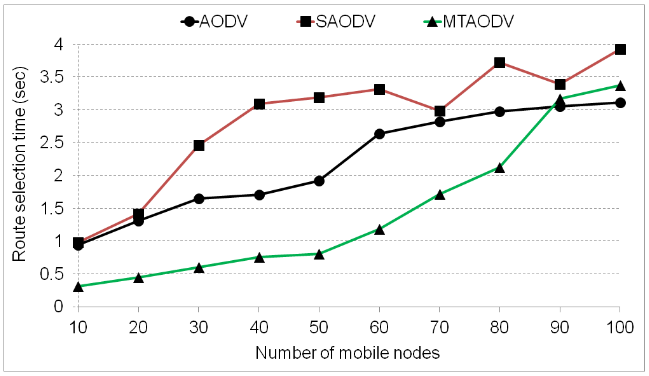

Figure 5: Effect on route selection time

6. Conclusion

AODV uses no security measures so is always prone to security threats. SAODV can fight various types of vulnerabilities of AODV. SAODV uses hybrid cryptography and provides security features such as integrity, authentication and non repudiation of routing data. The use of cryptographic approach that provides hop by hop security in SAODV again presents issues in routing performance in terms of routing overload and end to end delay.

Offering security only through cryptography is not always a suitable solution if the high dynamic context of MANET is considered. A trust mechanism that reduces the computationally intensive number of security operations becomes strategic. To improve performance of SAODV and offer more resilience to attack from malicious nodes authenticated by the network, a trust model must be added. Trust evaluation system can improve network throughput as well as effectively detect malicious behaviour in ad hoc networks. Network performance improves when sender node is able to skip malicious nodes based on trust values. The proposed mechanism for trust model implementation, M-TAODV is found efficient in terms of both routing efficiency and network resource utilization. Utilization of trust table to find out trusted route and to isolate malicious node before the actual communication was the reason for the improvement.

References

[1] L. Anil and G. Sohan. A study on the behavior of MANET: along with research challenges, application and security attacks. *International Journal of Emerging*

Trends & Technology in Computer Science, 4(2), April 2015.

[2] S. Anil and S. Poonam. Efficient techniques for SAODV in mobile ADHOC network. 2(8):42–49, August 2011.

[3] V. Manoj, M. Aaqib, N. Raghavendiran, and R. Vijayan. A novel security framework using trust and fuzzy logic in MANET. *International Journal of Distributed and Parallel Systems*, 3, 2012.

[4] K. Z. Bijon, M. M. Haque, and R. Hasan. A Trust Based Information Sharing Model (TRUISM) in MANET in the Presence of Uncertainty. In *12th Annual International Conference on Privacy, Security and Trust*. IEEE, 2014.

[5] M. K. Denko and T. Sun. Probabilistic trust management in pervasive computing. In *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC'08)*, pages 610–615, Shangai, China, Dec 2008.

[6] A. A. Pirzada and C. McDonald. Establishing trust in pure ad-hoc networks. pages 47–54, Dunedin, New Zealand, Estivill-Castro (Ed.), 2004.

[7] K. Z. Bijon, M. M. Haque, and R. Hasan. A Trust Based Information Sharing Model (TRUISM) in MANET in the Presence of Uncertainty. In *12th Annual International Conference on Privacy, Security and Trust*. IEEE, 2014.

[8] A. Lupia and F. De Rango. Evaluation of the energy consumption introduced by a trust management scheme on mobile ad-hoc networks. *Journal of Networks*, 10(4):240–251, April 2015.

[9] S. Pankaj and J. Yogendra Kumar. Trust based secure AODV in MANET. *Journal of Global Research in Computer Science*, 3(6):107–117, June 2012.

[10] K. Jaspreet and H. Sandeep. An Energy Efficient, Secure and Trust Aware Routing Protocol in MANET. *IJCSET*, 5(7):219–223, July 2015.

[11] J. Sen. A distributed trust and reputation framework for mobile ad hoc networks. In *Proceedings of the the 1st International Conference on Networks Security and its Applications*, pages 538–547, 2010.