Secure Timing Advance Based Context-Aware Handover Protocol for Vehicular Ad-Hoc Heterogeneous Networks

Vincent Omollo Nyangaresi¹, Dr. Silvance O. Abeka² and Prof. Anthony Rodrigues³
School of Informatics and Innovative systems
Jaramogi Oginga Odinga University of Science & Technology -Kenya

Abstract - Heterogeneous networks and their applications introduce new shortcomings in terms of access control and confidentiality during handover process. Unfortunately, implementing stronger security mechanisms during the handover process elongates the whole process as it increases the signaling traffic between the mobile units and the network. Handover authentication is a crucial process in heterogeneous cellular networks since it ensures that mobile nodes move across multiple access points utilizing different access technologies, securely and seamlessly. As such, a number of handover authentication algorithms and protocols have been developed while others have just been proposed. Unfortunately, the conventional handover authentication processes are susceptible to attacks owing to unsecured pre-authentication traffic. These attacks include jamming, denial of service and downgrade attacks which must be eliminated in order to strengthen the user’s security. In addition, current handover algorithms involve high signaling overheads, massive computation costs, call drops and call blocking. These call drops and call blocks may be occasioned by unavailability of free channels, low level of system configuration or high traffic densities. The effective handling of the handoff procedures reduces handoff failure rates, packet drop frequency and handoff latency. Consequently, the design of proficient handoff management techniques plays a significant role in providing the required quality of service to the subscribers. Since during the handover process the security mechanism may shift, the mobile equipment and the network must provide an assurance that they are able to communicate with each other only upon agreeing on the keys to be employed in the protection of their data. Past research has shown that handover failure is the main contributor to packet drops or call blocking. In this paper, an investigation of the various handover algorithms is provided and a critique of these algorithms is given. Based on the challenges of these handover techniques, a novel secure context-aware handover based on timing advance is proposed. The proposed protocol is hinged on mobile user mobility prediction and timing advance to preserve some time slots to facilitate the incorporation of strong authentication in the handover process.

Key words: Context-aware, Handovers, authentication, Hetnets, VANETS, timing advance, Fuzzy logic.

I. INTRODUCTION

The mobility feature of current phones has made mobile communication part and parcel of people’s daily lives, leading to their heavy deployment in private, business and critical infrastructure ecosystems. Increasingly, energy infrastructure, emergency services and payments services, have depended on cellular mobile networks.

Consequently, reliability and security aspects of these networks have attracted a lot of attention lately. In [1], it is explained that numerous security and privacy flaws have been established in mobile networks, some of which target the subscriber’s private data, mobile operator’s revenue or the availability of network resources.

In cellular networks, these handovers crop up when a subscriber roams from one network to another as shown in Figure 1.
In typical situations, a handover authentication process encompass three agents namely the mobile equipments (MUEs), access points (APs) and the authentication server (AS).

Normally, an MU has to register to the AS before establishing a connection to any AP to access its subscription services. In this scenario, an AP is a guarantor and is charged with the responsibility of vouching for an MU as a valid subscriber. In circumstances where an MU shifts from the present AP\textsubscript{1} into a new AP\textsubscript{2}, an execution of handover authentication at AP\textsubscript{2} needs to be activated. On its part, AP\textsubscript{2} has to confirm whether the MU requesting for handover to its region is an approved user and hence grant or deny access. Provided that the MU is a valid user, a session key is setup concurrently to offer protection for the communication between the MU and AP\textsubscript{2}.

With the advent of vehicular ad hoc networks (VANETs), the subscriber in bullet trains must be able to execute very fast handovers to avoid call drops. As [2] explain, there is a strong correlation between velocity and handover failures. This is occasioned by the fact that at high velocity, the duration across the handover region does not match the base handover delay. Consequently, the handover procedure cannot be accomplished in time and hence the call is terminated.

According to [3], handoff delay can lead to reduction in the quality of service in 4G networks that may influence the performance of both upper-layer protocols and applications. This can be alleviated by deploying a priority-based algorithm or utilizing location-aware adaptive applications.

As [4] point out, a number of issues are inherent in high velocity VANETs which include frequent handovers, Doppler recurrence movement and fast fading, large car body loss and multipath loss. Whereas frequent handovers lead to
regular cell re-selection, communication quality degradation, and data service unavailability, Doppler recurrence movements result into low communication connection rates, difficulties in handover initiation, and handover failures. On their part, a large car body loss and multipath loss, lead to weak intra-train signals. Frequent handovers are detrimental in mobile communication since they result into massive packet losses and packet reordering. Given the significance of the handover process in the provision of the best quality of service (QOS), it becomes important for the MU to decide on the location and time for carrying out a handover.

In their paper, [5] explain that heterogeneous networks (HetNets) have been introduced to cater for the ever increasing demand for high data transfer rates and traffic capacity. Each of the radio access technology has its own properties such as response time, coverage area and bandwidth. These features facilitate the deployment of applications and services that require large bandwidths, low latency, anywhere and anytime connection without experiencing disconnections.

Here, the mobility feature enables subscribers to roam throughout the network, connecting to a variety of radio access technologies. In legacy wireless networks, a single metric such as Received Signal Strength (RSS) is utilized as a basis for handovers. Handovers among a variety of radio access technologies constitute vertical handovers and a number of decision algorithms exist for these types of handovers. They include RSS-based, context-aware-based, cost function-based algorithms, fuzzy logic-based and multiple criteria-based algorithms.

In RSS-based algorithms, RSS threshold and the user’s velocity and location are utilized for handovers while in context-aware-based algorithms, the handover decision is hinged on signal quality, the network and the circumstance of the mobile device, where context can be take to be a situation of an entity or a location, environment, identity and time. In their research work, [6] discuss that cost function-based algorithms employ network-related cost function and user-related cost function, where user-related cost function may include security, monetary cost and power consumption. In fuzzy logic-based algorithms, a handover is executed in the two steps where the first step is concerned with fuzzification and weighting procedure while the second phase deals with decision making. As [7] illustrate, multiple criteria-based algorithms combine a number of metrics in the handover process to reduce power consumption.

Vertical handovers have proven crucial in facilitating seamless mobility and better QoS in networks. A number of current applications such as video conferencing, email, messaging and even TV require the connection to be sustained as the device move from one AP to another. They also enable a mobile user to shift the connection to another type of network. In [8], it is demonstrated that whereas horizontal handover takes place only when the RSS is feeble within the coverage area, vertical handover is based on users’ assessment and experience.

In their paper, [9] discuss that vertical handover process undergoes three phases namely handover information gathering, handover decision, and handover execution. Whereas the first phase involves the identification of particular information needed for justifying a handover process, the second phase deals with the establishment of the most suitable network access. The last phase occurs when an MU moves from its current network to the new network coverage. During the information gathering stage, data is obtained using three sources:
network detection in neighbor network, MU status, and user preferences. The first source employs metrics such as throughput, handover rates, cost, packet loss ratio, RSS, Noise Signal Ratio (NSR), Signal to interference ratio (SIR), Carrier to Interference ratio (CIR), bit error ratio (BER), distance, location and QoS. The second source uses battery status, speed, resources and service category while the third source utilizes budget, monetary cost and services.

According to [10], poorly designed handovers present a fertile ground for attackers to carry out their malicious activities. To uphold security, strong security mechanisms should be put in place during this process. Unfortunately, a number of messages that are exchanged before the authentication and key agreement form the root cause of multiple attacks.

II. RELATED WORK
The sporadic change in the MU’s velocity has been established to a major cause of poor handover quality that may lead to massive packet losses and hence denial of service. In order to alleviate this problem and at the same time reducing ping pong handovers, [11] applied Allan variance to the RSS received from the serving AP to detect any variations in velocity and were able to fine tune handover parameters for each MU based on its velocity and the coverage area of AP. This approach resulted in accurate velocity prediction, reduced the number of ping pong handovers and handover failures.

In HetNets, there is a need for the subscribers to be connected to the best network at any given time to get higher data rates. A major challenge here, especially for high velocity users, is how to execute the handover as quickly as possible. For this to happen, the velocity of the MU must be known and various radio access technologies must be compatible with each other to guarantee the best QoS. To address this challenge, media independent handover (MIH) has been proposed by [12] to provide a mobility process which is autonomous to the media. This MIH should be capable of availing link layer data as well the optimum target networks.

Given the significance of subscriber velocity estimation, there has been research on portable velocity estimation. As a result, the authors in [13] have developed a handover count-based technique that is correlated to velocity estimation. Basically, the MU’s mobility is assessed using the number of handovers it executes within a given time frame. This approach has been applied in Long-Term Evolution (LTE) and LTE-Advanced (LTE-A) to categorize the mobility situation of the MU into three large classes namely low, medium and high.

Prolonged handover delays can lead to denial of service hence compromising availability of network resources to the subscribers. As such, [14] explain that tracking velocity can reduce both handover delays and number of handovers within a particular time window. Consequently, handover algorithm execution can be improved. In their study, [15] illustrated that low quality in handover execution results in severe interruption and call drops. Velocity-based methods for handover triggering have the ability of lessening call drop rates, more so in high velocity VANETs, leading to enhanced handover performance.

In their paper, [16] proposed a novel design of handover authentication for HetNet mobile cloud networks that offers user anonymity and untraceability. It was shown to achieve enhanced universality, strong security and efficacy, hence helped address handover security and privacy in Mobile Cloud Computing (MCC) technology.
An enhanced vertical handover decision algorithm based on multiple criteria in the heterogeneous wireless network has been proposed by [5]. The algorithm encompasses three technology interfaces namely LTE, Worldwide interoperability for Microwave Access (WiMAX) and Wireless Local Area Network (WLAN). In addition, this algorithm utilizes three types of vertical handover decision algorithms namely equal priority, mobile priority and network priority. In terms of handover number and handover failure probabilities, the simulation results showed that these three algorithms were superior to the conventional network decision algorithm. Amongst themselves, the network priority handover decision algorithm achieved the best results compared to the other two.

The authors in [17] developed a new pairing-free handover authentication technique for mobile wireless networks. This scheme was shown to be advanced in terms of mutual authentication and resistant to network threats, and involved lower computation and communication costs. On their paper, [18] proposed a handover authentication scheme named Pair-Hand, which they stated can was resistant to various attacks.

However, no rigorous security verifications were provided to support this. Based on bilinear pairings and identity (ID)-based signature, [19] designed an anonymous mobile node handover authentication (AMNHA) protocol that employed a pseudo-ID to offer mutual authentication and privacy protection among communication entities. It permits an MU to roam seamlessly over multiple APs in mobile networks while offering mutual authentication hence protecting the privacy of MUs.

A research work by [20] proposed a vertical handover decision algorithm that utilized a fuzzy logic algorithm. The goal of this algorithm was to boost QoS in HetNet VANETs. The results indicated that this algorithm performed well compared to the conventional RSS Threshold algorithm in terms of average percentage of handover QoS parameters such as handover latency, delays and packet losses.

As [21] explain, a number of schemes have been proposed to address the challenges of handover failures and call drops. These techniques include guard channel prioritization schemes, utilizing auxiliary stations (AuS) and handover queuing prioritization schemes. In the first scheme, a given number of channels are reserved specifically for handovers while the rest of the channels are shared between fresh calls and handover calls.

In the second technique, a base transceiver station (BTS) has two or more auxiliary stations such that when a call arrives at the BTS, it is initially served by the AuS provided it has free channels. When free channels are detected at the BTS, the call can be shifted from the AuS to the BTS. In the last scheme, a queue is created for all handover calls such that upon the detection of a free channel, it is assigned to the handover call in the queue in a first in first out (FIFO) basis. This technique works in BTSes overlapping regions where an MU is capable of communicating with more than one BTS. Queuing handover calls reduces call dropping resulting from handover failures. Here, whenever the call’s RSS reaches a certain set threshold, it is added to the queue. Unfortunately, if a call is queued and no free channel is released, the call is effectively blocked by the BTS.

In their study, [22] suggested an efficient and secure handover authentication scheme based on elliptic curve cryptography. This scheme was shown to be resistant against key compromise attack, attain forward secrecy and
anonymity, and efficient in terms of communication and computation costs.

III. CRITIQUE OF CURRENT HANDOVER AUTHENTICATION

In this section, a critique of the conventional as well as the proposed handover authentication algorithms is provided based on the three goals of security: confidentiality, integrity, privacy and availability. Impersonation attacks can make unsuspecting communication entity to reveal private information, compromising confidentiality and privacy goals while traffic redirections to fake base stations can lead to modification of data before forwarding these data to the receiver, compromising integrity of the communication process. Massive packet drops, signaling overhead exchanges, call blockings and prolonged delays during handovers can easily lead to denial of service and therefore compromise availability goal.

Ideal handovers authentication schemes and algorithms can ensure a seamless network access control and as such, a number of researchers have paid attention to this area. Unfortunately, a number of the existing and proposed techniques and algorithms fall short of expectations in one aspect or another. For instance, smart-card based handover authentication scheme proposed by [18] requires that AP₂ contact an AS to establish the MU’s authenticity. In this process, when an MU shifts from AP₁ to AP₂, four messages are exchanged among the MU, AP₁ and AP₂, which result in massive computation and communication delay more so when an AS is remotely located.

To improve on the first scheme, [18] proposed another privacy preserving handover authentication technique that eliminated the need for AP₂ to communicate with AS. However, this still called for three messages to be exchanged between an MU and AP₂ for key establishment and mutual authentication. Later, these authors proposed a Pair-Hand scheme that eliminated the participation of AS and only required two handshakes between an MU and AP₂ for key establishment and mutual authentication. This scheme was meant to improve communication efficiency, lessen the load on AS and protect subscriber’s privacy by use of short-lived pseudonyms. Unfortunately, the proposed scheme is prone to private key compromise attack, making it feasible for an attacker to retrieve any MU’s private key.

To strengthen Pair-Hand, [18] replaced the prime q order bilinear group with a composite n order bilinear group. As described by [23], this scheme is still susceptible to private key compromise attack. In addition, an attacker can compute the master key in circumstances where the prime factors of n are moderately small, and the authors could not propose any effective remedy against these attacks.

In their paper, [22] further showed that Pair-Hand can never guarantee forward secrecy and strong anonymity, and is susceptible to key compromise attack that enables an intruder to recover the private key of any MU. To address this problem, [24] and [25] proposed two handover authentication techniques derived from the prime-order bilinear pairings. These schemes were resistant to private key compromise attack but could not attain forward secrecy. Additionally, these techniques are susceptible to known session key attacks.

In their paper, [26] proposed a handover authentication scheme devoid of bilinear pairings, which [27] showed that it is prone to access point impersonation attacks. The authors in [28] investigated a number of target cell selection criteria such as RSS and available bandwidth that
they thought would boost handover success rates and lessen call blockings and hence improve the quality of video and multimedia traffic delivery. These authors then proposed a handover triggering technique based on the quality of the received multimedia information. The demerit of this technique is the difficulty encountered in the estimation of the correct quantity of multimedia data for triggering a handover.

As pointed out by [29], although a number of HetNets authentication protocols have been proposed for the purpose of ensuring a secure and proficient handover authentication, these protocols have a number setbacks. The first issue is the need for the interaction with an AS during the mutual authentication process, or the participation of third parties such as APs and BTSes. In addition, these schemes are cumbersome in their design making them incompatible with each other. They also have security flaws that expose the subscribers’ private data, incur high authentication costs leading to low efficiency and cannot assure seamless handovers.

A Universal Subscriber Identity Module (USIM) based authentication test-bed for the Universal Mobile Telecommunications Systems (UMTS)-WLAN handover has been proposed. Unfortunately, there is no elaborate description on how fast authentication and handover authentication can be achieved. In addition, the performance of the proposed fast re-authentication does not meet the requirement of delay-sensitive application. A pre-authentication based scheme that generates master session keys when a subscriber first logs in the network and sends these keys to the target network when necessary has been suggested for Wireless Fidelity (WiFi) and WiMAX integrated network. This technique localizes the handover authentication process hence simplifying it since it requires only message flows between the MU and the target BTS or AP without the involvement of an AS. A similar authentication scheme based on key reuse has been proposed to decrease the processing time for key-reuse during handover, and alleviate frequent handovers between two BTSes. However, the performance analysis demonstrate that both of these techniques may encounter delayed authentication when the master key misses or the MU moves to a target AP or BTS that has not received the key.

This leads elongated authentication latency. A one-pass authentication and key agreement (AKA) technique that reduces authentication costs through the usage of an international mobile subscriber identity–IP multimedia private identity pair has been proposed for 3G-WLAN integrated networks. On the flip side, the security analysis reveals that the users are susceptible to spoofing attacks from rogue third party application vendors.

In [5], the authors discuss that vertical handover triggered by only one criterion such as RSS may lead to service interruption, an unbalanced network load and an inefficient vertical handover. This is because RSS fluctuates and hence unreliable. The root cause of this problem is that each element in a HetNets has different thresholds of RSS, resulting into high packet delay, excessive handovers, high handover failure probability and this diminishes overall throughput in the RSS-based algorithm.

The unnecessary handovers and dropped calls may be prompted by low signal quality or the long distances between the MU and the AP or BTS. These challenges are pronounced in overlapping regions where users travel quickly back and forth between one cell and the next cell. Further, [20] discuss that RSS based handovers deteriorate handover performance due to increased handover latency, delay,
dropped calls, packet loss, and handover failure probability. These handovers are only ideal for horizontal handover decision to ensure QoS and not in vertical handover decision in advanced technologies since in next generation networks, vertical handovers can be initiated based on the subscriber’s convenience or preference rather than connectivity reasons.

On their part, fuzzy logic and cost function algorithms are highly accurate and efficient but are also very complex to implement. Context-aware based algorithms have high throughput but experience long handover delays. On their part, multiple criteria based algorithms have low handover failure but have no support for fuzzy decisions.

According to [17], handover authentication protocols based on a bilinear pairing mapping present an exercise that is time consuming and inefficient, making them inappropriate for practical circumstances. On its part, a secure and efficient roaming AMNHA protocol is cumbersome to design due to the broadcast nature of wireless networks, the limited power and resources of MU’s.

This protocol is also insecure and susceptible to key compromise attacks. As [25] explain, AMNHA protocols based on bilinear pairings and elliptic curve cryptosystem (ECC) require complex and time consuming activities, making them inappropriate for deployment in a mobile environment because MU’s have limited power and processing capability. To alleviate these shortcomings, several pairing-free techniques have been suggested that completely do away bilinear pairing operations.

It is discussed in [27] that one of such protocol is an identity-based AMNHA protocol that minimizes message exchanges while at the same time ensuring strong security. Unfortunately, this scheme is susceptible to attacks and hence insecure. The authors then proposed a dynamic multi-attribute network selection algorithm to facilitate user mutual authentication and hence ensure enhanced security and efficiency in vertical handover procedures over mobile ad hoc networks (MANETs).

However, as [26] point out, this improved technique cannot guarantee user untraceability and anonymity since the actual identity of the MU is sent in plain text over the wireless networks. Afterwards, [26] suggested a privacy-aware AMNHA protocol that adopted identity-based cryptography and pseudo-ID for the MU. This protocol was shown to be secure under an extended Canetti–Krawczyk model, had good performance and attained user anonymity. On the flip side, [27] and [30] showed that this protocol is susceptible to fraud attacks and is unable to offer mutual authentication between an MU and an AP. This then enables an adversary to impersonate a legitimate AP and establish a communication with an unsuspecting MU.

To address this problem, [29] presented a new privacy preserving AMNHA scheme devoid of pairing operations. The technique was shown to assure robust security and efficiency while at the same time supporting user anonymity and untraceability. Nevertheless, [17] demonstrated that this scheme is vulnerable to MU impersonation attack that can lead to failure of mutual authentication.

IV. REQUIREMENTS FOR THE PROPOSED HANDOVER

A review of the existing and proposed handover authentication algorithms has shown that they face various challenges in their operations or implementations that compromise confidentiality, integrity, privacy and availability. Based on these weaknesses, a new timing advance context aware handover algorithm is proposed. In
this section, the requirements of the proposed protocol are provided.

Seamless network connections are only feasible when the handover decision algorithm possess enough intelligence to enable it decide the best candidate network by taking into consideration multiple parameters related to the intricacy of current network architectures and technological advancements. Since the choice of an appropriate metric for the handover process is crucial for the handover accuracy, a number of criteria that are both user related and network related will be utilized, which include velocity, traffic densities, multi-path fading, power requirements, in signal-to-noise ratio (SNR), interference, QoS, cost of service, user preferences, RSS, mobility, application and bandwidth.

As such, this handover will be multivariate in nature so as to provide an alternative network that is the best target when other metrics are equal among the candidate cells. Currently, it is a challenge to implement this kind of vertical handover decision algorithm due to the short time that is available for the handover process.

Velocity criterion will be instrumental for high speed users to thwart any ping pong handovers since velocity and frequency of handovers are strongly correlated. In very small cells, high velocity users spend very little time in these cells such that no enough measurement data is gathered.

Since natural interference, multi-path fading, and signal-to-noise ratio may lead to instability in the link quality, hence affecting the growing subscribers’ demand for entertainment applications such as high-speed Voice-over-IP (VoIP) and Internet Protocol TV (IPTV) services during traveling, these variables must be factored in during the handover process.

Security and efficiency are other requirements that the proposed protocol should strive to achieve. The proposed handover should achieve both functional and informational security. Whereas functional security is concerned with the proper operation of the handover procedures, informational security deals with data and location confidentiality, access control and data integrity. Consequently, functional security is concerned with handover aspects such as availability, reliability and maintainability that protect the handover process from malfunctions. The handover authentication process should be designed in such a way that it becomes fast enough to cope with time constraints of handover. His can achieved through next cell prediction facilitated by MU mobility prediction.

Since MU’s are constrained in terms of energy supply, bandwidth and processing capability, the suggested handover should be as network controlled as possible. All the information about the signal quality for all MU’s should be available at a single repository in the network and the network should be context-aware such that it periodically makes measurements to determine both MU and network status at various locations within the coverage areas.

This will ensure regular network paging that will ultimately reduce the timing advance, making the handover process and the authentication process as efficient as possible in terms of communication and computation. The reduced timing advance can then be utilized as a trade-off for the proposed multivariate handover and its authentication process, which helps it to attain informational security objectives of data and location confidentiality, access control and data integrity.

Another important necessity of the proposed handover is that it should permit the MU to roam seamlessly across the
HetNets enjoying full connectivity. Since security policies in various radio access technologies vary greatly, the suggested handover algorithm should be capable of resolving the security contexts a fresh upon a vertical handover. This is an issue that diminishes efficiency and induces security risks in the current handovers. In addition, the proposed protocol should be context aware in the sense that it should be intelligent enough to detect diverse mobility, QoS and security requirements of the various radio access technologies. This is a difficult exercise in the conventional handovers that derail the support for seamless roaming and secure handovers.

With the advent of real-time cloud applications exemplified by video conferencing and media streaming that have strict performance requirements in terms of end-to-end delay and packet losses, the proposed protocol should be efficient enough to prevent DOS that may be occasioned by long delays and massive packet losses.

Since strong authentication algorithms are needed to prevent impersonation and eavesdropping attacks that may facilitate data modification hence compromising confidentiality and integrity, this protocol should be capable of ensuring that all MUs are properly and efficiently verified before being handed over. This will involve digital certificates exchanged among three entities namely the MU, BTS\(_1\) and BTS\(_2\).

In addition, a strong encryption algorithm should be employed to generate session keys to be utilized among the authenticated entities to boost confidentiality and integrity of the communication session. Some of the data that should be protected include MU location and identities exchanged during handovers. This is geared towards the prevention of impersonation attacks that may be feasible by the leakage of this data. Conventional roaming protocols have been shown to expose user identities and locations during the authentication phase, hence making it possible for adversaries to track users.

The proposed HetNet handover authentication protocol should be reliable, accurate and able to distribute MUs fairly among the cells to ensure load balancing. This is significant to thwart BTS breakdown that may be occasioned by heavy traffic loads.

V. ALGORITHM DESIGN

The proposed handover protocol should be designed in such a way that it achieves the security goals of confidentiality, integrity, privacy and availability. By implementing network based intelligence gathering, MU mobility prediction and regular paging, timing advance is reduced and this extra time obtained can be utilized to realize strong authentication during handover.

The first design component of the proposed handover is a buffer to queue the handover calls as the source BTS and target BTS exchange MU details and the target BTS authenticates the MU. This effectively prevents call drops that result when the target BTS has no free channels. Although call drops can also occur due to low level system configuration settings, radio frequency (RF) call drops and handover failure call drops are the most predominant. Buffering reduces call drops and packet losses, helping the proposed protocol to achieve functional security goals of availability, reliability and maintainability of the handover process.

Radio frequency call drops occur due to downlink and uplink failures occasioned by severe interference that make it impossible for the MU to decode the slow associated control channel (SACCH). Since SACCH carry system information necessary for call establishment, when the
MU fails to decode it, the radio channel is connection is released suddenly resulting in dropped calls. Power failure, hardware failure, improper radio parameter settings, intra-network interference and weak radio signals within the coverage area are other reasons for RF call drops.

Handover failure call drops crop in when the MU receives a handover command but fails to perform this handover to the next cell, and at the same time it cannot communicate with the original cell. As such, the MU is disconnected from the network and the handover control timer at the BTS informs the mobile switching center (MSC) of this failure which then releases the channel.

The second component is the network topology sensing unit (NTSU) that is charged with topology mapping. The proposed protocol should operate in a HetNet consisting of LTE, WiMAX and WLAN networks. Whereas the WiMAX will cover the largest radius, LTE will occupy much a smaller radius and WLAN will cover the least radius of the simulation area.

The third component is the fuzzy inference unit (FIU) that will be responsible for selecting the best target networks that provides least handover delays and packet losses.

The fourth component is the context repository (CR) that will gather and hold both user and network status of all the handover parameters. All the networks in HetNets consisting LTE, WiMAX and WLAN should contribute variables to act as inputs to the fuzzy logic unit. The fifth element is the mobility prediction unit (MPU) while the sixth component is the certificate authority (CA) that will be charged with authenticating the MU, the source BTS and the target BTS.

VI. EXPERIMENTAL DESIGN
The proposed handover shall be implemented in a VANET HetNet consisting of LTE, WLAN and WiMAX. This shall necessitate the partitioning of the network coverage area such that each of these access technologies occupies a certain radius of the total coverage region as shown in Figure 2.

![Figure 2: Proposed Vertical Handover in VANET HetNet](image)

As this figure demonstrates, a vehicle should be meant to move across all the three radio access technologies, starting at the WiMAX coverage area and finishing at the LTE coverage area. Since the APs and BTS in these radio access technologies have antennas that radiate radio signals omni-directionally, these signals get attenuated as the distance from the access points increases, handovers become necessary.
Apart from the conventional RSS, other metrics discussed above should be incorporated in the handover process.

VII. HANDOVER OPERATION

The handover decision process begins with the FIU receiving context handover metrics (CHM) from the CR. It then evaluates these metrics using the rules in the fuzzifier to suit the user’s as well as the network conditions. The third phase was the fuzzification process where the metrics should be transformed into membership functions (MFs). The proposed protocol will consist of five membership functions namely weak, average, strong, available and unavailable as shown in Table 1.

<table>
<thead>
<tr>
<th>Membership Functions</th>
<th>Weak</th>
<th>Average</th>
<th>Strong</th>
<th>Accessible</th>
<th>Inaccessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

The variables in the context repository should be scaled and partitioned to yield the values in Table 1 above. As an illustration, the traffic densities (TD) can have a range of between 1 and 10 Erlangs, and SNR can range from 0.1 to 0.5, which are then portioned as shown in Table 2.

<table>
<thead>
<tr>
<th>TD(Erlangs)</th>
<th>Weak</th>
<th>Average</th>
<th>Strong</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD &lt; 3</td>
<td></td>
<td>3 ≤ TD &lt; 7</td>
<td>TD ≥ 80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNR (dB)</th>
<th>Weak</th>
<th>Average</th>
<th>Strong</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNR &lt;0.2</td>
<td></td>
<td>0.2 &lt; SNR &lt;0.4</td>
<td>SNR &gt; 0.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User service Types</th>
<th>Inaccessible</th>
<th>Accessible</th>
<th>Accessible</th>
</tr>
</thead>
</table>

The fourth step involves the membership function establishing the network links status (NLS) and passing its results to the comparator residing in the defuzzification unit (DU) in the fifth phase. During the sixth step, the handover execution unit (HEU) takes as input the outcome of the DU and hands over the MU to the target cell with the best membership function. Figure 2 shows the design of the timing advance secure context-aware handover protocol (TASCAHP).

As Figure 2 shows, to achieve functional security, target cell prediction through MU mobility prediction, and periodic network paging (PNP) should be carried out. By saving time during the handover preparation phase, timing advance can be reduced. This should save some time slots that can be employed to integrate strong authentication through digital certificates via certificate authority (CA), which in turn can help implement tight access control which thwarts adversaries from eavesdropping, impersonating MU’s or redirecting traffic to fake BTSes. Ultimately, this helps attain informational security goals of data and location confidentiality, access control and data integrity.

Based on the fact that whenever an MU connects to a network AP it establishes a security context with a provider, then during the handover procedures, some or the whole network elements involved in the securing the communications may change. Consequently, the current security context has to change as well. This means that the MU and the network have to agree upon the encryption keys to be used for communications protection to guarantee that packets exchanges are still secured.
During a group call, the Group Receive Mode (GRM) specification points out that the listening MU is in idle mode and as such, data measurement required for handover preparation takes a long time. For instance, an MU may take fifteen seconds attempting to decode parameters while the computation of the mean of five measurement samples spread over three to five seconds may take at least the three seconds.

On its part, the BTS identity code can be decoded in every ten seconds while the Broadcast channel may be decoded at least every thirty seconds. Depending on provider and field strength requirements, networks with high reliability and availability requirements and with MUs’ traversing the network at high velocities result into small cells with a diameter of two to three kilometers. Consequently, an MU stays in the same cell for a limited period of time. In worst cases, no measurement takes place when an MU crosses a given cell.

Handovers problems in high velocity users can be solved by making the handover procedures as fast as possible. Mobility prediction that can facilitate the identification of the next cell the MU is likely to move to, together with regular base station controller (BSC) MU paging can be employed to achieve this. This requires the knowledge of network topology, location and direction of the movement of the MU. High velocity subscribers tend to form a special movement pattern, assuming linear movements along motorways and tracks, with the shape of the planning area shifting from area-wide to a line-shaped grid. This information is crucial and can be employed to execute a handover with little or no measurement effort at all.

To put this into context, assume an MU is moving in a straight line, traversing from area covered by BTS$_4$ towards BTS$_1$. Let us make other assumptions that there are no turnarounds since this MU is moving at high velocity, and that each BTS has only two neighbours as shown in Figure 3.
Then for this MU to reach area covered by BTS₁, it has to leave the areas covered by BTS₂ and BTS₃. In this situation, the next candidate cell can be easily predicted from the knowledge of the previous locations of the MU. In regions with many crossings, if the MU changes direction, then the velocity would not be so high and the usual handover procedure can be implemented.

In overlapping regions, coverage can be provided by either neighbouring BTSes or by a special transmitter located in these regions to prevent handover failures. In both scenarios, the direction of movement of the MU has to be predicted. The distance between an MU and the BTSes can be obtained from the timing advance values. For the case of the network topology of Figure 3, the direction of the MU can be derived from the knowledge of the last serving cell, and this information can then be forwarded to the target new serving cell during the handover process. Using this information, the new serving cell can predict the cell for the subsequent handover straight away.

The above described mobility prediction fails when there are more target cells for the MU to handover to. In this case, the incoming direction intelligence about the last serving cell is not sufficient and the MU may be required to provide more measurement information such as location reports. The tedious task here is to extract that exact location of the MU. Considering the network topology of Figure 4, the location data can be obtained from timing advance measurement of three BTSes with contact to the MU. For the case of line-shaped networks, two BTSes are adequate to compute location data given the knowledge of the motion track and this reduces the measurements for the MU.

In the proposed handover authentication protocol, the BSC should be charged with the responsibility of the handover process. In this case, if the BSC is aware of the direction and location of the MU within the network, then it can either force the MU to perform a handover to the next candidate cell at a certain point in time, based on the metrics suggested in this paper.

Having predicted the next target cell, another challenge is to decide the time at which authentication process should be carried out in the handover process. In mobile telephony, authentication process takes place before location updates and before call setups.

Figure 3: VANET Network Topology
Due to the time restrictions during the handover process, the same authentication and key agreement procedures cannot be implemented in the usual way while the connection between MU and the target BTS is established. For instance, the global system for mobile communications (GSM) limits the time between the handover command and the handover completion or failure message to between 0.5 and 1.5 seconds. Unfortunately, the generation of a handover authentication response can take the MU up to 0.5 seconds and as such the connection would be interrupted by this additional authentication.

Fortunately, the periodic paging and mobility prediction this paper can reduce the signaling messages exchanged between an MU and the previous BTS and hence the free time slots so created can be utilized to forward authentication messages between the MU, the previous BTS as well as the new BTS as illustrated in Figure 5.

As shown in this figure, the BSC should in charge of generating measurement reports
while the MU carries out the pre-computation of authentication challenge, encryption and integrity keys before the actual shift of channel. At the time when an MU and the new BTS have setup a connection, an MU transmits the pre-computed authentication response and the new BTS verifies it. Provided that this authentication response is valid, handover complete message is transmitted and the old BTS releases the radio resources, otherwise a handover failure is transmitted and the MU falls back to the old channel.

VIII. PROPOSED HANDOVER PROTOCOL FLOW CHART

The proposed handover protocol will go through a number of steps before a final handover decision is made concerning the selection of the most ideal target network as shown in Figure 6. The handover process will start off by having the protocol initialize the network topology which shall consist of LTE, WiMAX and WLAN.

This will be followed by the initialization of the MUs and mobility pattern that shall be employed to depict subscriber movement within the network coverage area and hence plays a crucial part in predicting the next cell that the MU will shift to. The next phase shall be the measurement and computation of all the handover metrics envisioned in this paper.

After this, the protocol shall be ready to create a set of all the networks that the MU is eligible to be handed over to. In circumstances where there is a single network, then the MU will not handover and hence will be retained in the current cell. However, if there is more than one network on sight, the proposed fuzzy logic and authentication shall apply and the MU is handed over to the next cell. This flow chart also includes the conventional RSS based handover that shall be utilized for evaluation purposes.

The operation of the strong authentication process will be facilitated by the usage of digital certificates that will be exchanged among the original serving BTS, the candidate target BTS and the MU to be handed over.

IX. PROTOCOL EVALUATION

A number of parameters shall be employed to evaluate the developed protocol to gauge its network performance. These parameters shall include bit error rates (BER), handover success rates, number of handovers per unit time, end to end delay, handover failure probability, handover latency, jitter, packet loss, handover failure rates, and bandwidth.

Since RSS based algorithm is cost efficient, simple and all mobile phones can measure it, this is the algorithm employed in most real deployments. As such, to investigate the effectiveness of the proposed handover protocol, the simulations shall be carried out using RSS as the benchmark. This shall require the design and implementation of a conventional handover using RSS in HetNets. Afterwards, comparisons shall be carried out using the parameters above to determine the best option.

In accessing mobile network’s performance, the number of vertical handovers during a given call is important since it affects the signaling load and QoS. Unnecessary handovers wastes radio resources, time and hence lead to inefficiency. On its part, handover failure probability represents the average incoming handover requests that cannot be completed due to the lack of free channels.

Handover latency represents the time taken for a data packet to be transmitted from the source MU to the receiver MU and hence may include the processing time at the MU’s. On the other hand, end-to-end delay or one way delay is the time taken for a packet to be sent across a network from
the source to the destination. Packet loss refers to the total number of packets that could not reach their destination during the handover process.

X. CONCLUSION
In this paper, a number of handover algorithms and handover authentication schemes have been reviewed and their shortcomings pointed out. Thereafter, a timing advance secure context-aware handover protocol for vehicular ad-hoc heterogeneous networks was proposed. The requirements of this protocol, its design both logical and experimental, its handover authentication process, overall protocol operation, flow chart and evaluation metrics have also been discussed. Future work in this area is the implementation of the proposed protocol.

Figure 6: Proposed Handover Protocol Flow Chart
in a heterogeneous VANET environment. It will also be important to run the actual simulations in order to compare the performance of the proposed protocol with the conventional RSS based handovers.

REFERENCES


