DRDC-RDDC-2016-P118

A Prototype Implementation of Continuous Authentication for Tactical Applications

J. David Brown, William Pase, Chris McKenzie, Mazda Salmanian, Helen Tang

{david.brown, mazda.salmanian, helen.tang}@drdc-rddc.gc.ca
bill@armacode.com, chris@mckenzieic.com

Abstract. Recent advances in wireless and computing technology have led to accelerated efforts to equip soldiers at the tactical level with sophisticated handheld communications devices to share situational awareness data. An important consideration is how to secure these devices, and how to ensure that the users of the devices have not been compromised. This paper presents the details of prototyping activity we conducted in which two commercial biometric devices were integrated with a handheld communication device to perform continuous user authentication. We discuss the design of the prototype, its performance, and lessons learned that apply to future efforts at implementing continuous authentication in a military-focused setting.

Keywords: Continuous authentication, mobile ad hoc networks, biometric authentication.

1 Introduction

The concept of a networked soldier has been a part of military doctrine for years [1-4]. With recent advances in commercial and military technology, in the near future dismounted soldiers will be equipped with handheld networked computing devices to provide geographic situational awareness and to provide communications and information sharing capabilities during tactical operations. To ensure the integrity and confidentiality of the data on the communications devices, some form of user authentication is required such that a user can authenticate to his or her device. Additionally, it is desired that beyond a one-time user-to-device authentication, the trust relationship between user and device can be maintained through some form of continuous user authentication. The need for this continuous authentication is especially relevant in tactical operations, where users may be operating in contested or dangerous environments and are faced with a significant risk of device loss or capture by an adversary.

In this paper, we discuss the design, implementation, and evaluation of a prototype in which we integrated two commercial biometric devices with a smartphone operating in a mobile ad hoc network (MANET). The first biometric device measured the user's electrocardiogram (ECG) reading and the second measured the user's pulse. While many of the more common authentication techniques currently being explored in the literature may have significant value for commercial applications, this paper discusses how those techniques are less applicable in a military setting. Specifically, the contribution of this paper is twofold:

1) the paper details the military-specific constraints that place serious real-world limitations on the types of continuous authentication techniques that would be useful and feasible in a tactical edge scenario; and
2) the paper demonstrates—with prototyping, integration, and experimentation—the feasibility of a practical method for continuous user authentication that could operate under (a subset of) the constraints imposed by a military tactical networking use case.

A variety of techniques for continuous user authentication have been proposed in the academic literature, where these are often based on monitoring one or more of a user's biometric features. Initial variants of this work considered the case of a user sitting at a desktop computer and focused on monitoring data such as keystroke timing—see, for instance [5] for an early discussion of this style of continuous authentication, or [6, 7] for more recent iterations on this theme. Exploring user mouse dynamics was seen as a promising technique for the desktop user as well, as reported in [8]. For mobile devices such as smartphones, however, keyboard and mouse techniques are not applicable, and recent studies have focused on using elements such as touch-screen interactions or leveraging the outputs from on-board gyroscopes or cameras to develop a reliable biometric. Promising results have been obtained using touch-screen interaction for continuous authentication, looking at how a user swipes, "pinches to zoom", or performs other touch gestures; these gestures are compared to a stored template as in [9] or to data learned dynamically during the session as in [10]. The possibility of using a smartphone's on-board motion sensors to identify users and/or perform continuous authentication is explored in [11], but it is clear that there is still more work to be done to make such a system robust. In [12], the authors combine motion sensing with images observed by the on-board camera in an attempt to increase the reliability of a motion-based system.

Despite the promise of the continuous authentication techniques proposed in [5-12], their applicability to a tactical military environment is limited. Keyboard- or typing-based techniques are not useful since dismounted tactical users are unlikely to have keyboards. Touch screen-based techniques have limited value since users are not expected to be interacting frequently enough with the device for this technique to ensure "continuity" (i.e., there will be large gaps in time where the user will not touch a screen); additionally, users will likely be wearing gloves, which will reduce the sensitivity of any such algorithms. Examining output from the onboard gyroscopes still requires more robustness; furthermore, in a military setting, users can be expected to move in unpredictable ways, which could complicate generating a "template" of user behaviour. The high tempo and unpredictable nature of tactical operations necessitates a non-intrusive method of performing continuous authentication.

In this work, we consider two commercial sensors worn on the user's wrist; one measures a user's ECG reading as a means of providing strong initial authentication, and the other continuously measures the user's pulse as a means of providing "continuity". The possibility of using ECG data as a means for user authentication has been a topic of study for some time. In 2001, [13] showed that ECG data collected from a 12-lead ECG on individuals at rest was sufficient to perform user identification, correctly identifying better than 45 individuals out of a group of 50.

The effect of anxiety and stress on the accuracy of ECG identification was explored in [14], which showed that high-resolution ECG data provided a reliable means of user identification for individuals at rest and for those performing in high anxiety situations, with a better than 90% correct identification rate. Work by a number of researchers, including [15, 16], has focused on methods to improve the accuracy of performing user identification through ECG and has achieved success rates above 95%. Taken together, ECG and pulse measurements are a potentially attractive biometric combination since they also provide a proof-of-life indicator, which is vital in contested military environments.

The remainder of this paper is organized as follows. In section 2, we discuss the implementation details of our prototype, including the devices we used, how they were integrated with a custom smartphone application (app), and how they—in combination with the app—performed continuous authentication. Section 3 details the testing and evaluation of the prototype; we show the results of experiments run to measure the average time to detect a "lost device" and the average time to detect a "compromised" user. In section 4 we provide discussion and lessons learned from this exercise, including notes on how such technology could be modified in order to be better suited for a tactical operations use case. We sum up with a brief conclusion in section 5.

2 Prototype Implementation

We developed a prototype implementation that provides continuous authentication functionality for the particular use case of a dismounted soldier operating in a tactical environment. Our basic assumptions were that the user was equipped with a portable communications device consisting of a small graphical user interface display and a radio for short-range communication. In this use case, it is desirable (and practical) for the user to authenticate to the device only once—upon power up at the beginning of the mission. Thereafter, the device should remain active and should not "lock" even if the user has not interacted with the device for several minutes; it is impractical for a user in a tactical setting to re-authenticate once a mission has begun. In the absence of locking or re-authentication, a continuous authentication system should detect if the user has lost the device (i.e., detect a dropped/stolen device) or if the user has been compromised (i.e., detect loss of life).

For our prototype, we used a Nexus 5 smartphone with an external 802.11 transceiver to serve as our tactical communications device. The smartphone communicated using ad hoc 802.11 with other similarly-configured devices as part of a mobile ad hoc network. We integrated two external devices with the smartphone: 1) the "Nymi band", a commercial wristband produced by Nymi Inc. (see [17]) that measures a wearer's ECG reading; and 2) the "MIO LINK", a commercial wristband produced by MIO Global (see [18]) that measures a wearer's heart rate. The outputs of the Nymi band and the MIO LINK were fused by a custom Android app we created to detect a lost device or a compromised user.

Out of the box, the Nymi band operates as follows. A user completes an enrollment process (only required on first use) in which the user wears the wristband

and uses a company-provided "companion app" to assign a password and provide training data of the user's ECG reading (performed by the Nymi wristband). Whenever the user subsequently puts on the Nymi band, the user must complete an "activation" step, which consists of the Nymi band running an ECG measurement and validating (through the "companion app") that the correct user is wearing the band. Once the band is activated the user no longer needs to re-activate the band unless the band is removed. Note that this is an important security feature provided by the Nymi—the fact that wristband removal is detected ensures that (in most use cases) the user who authenticated is still the user wearing the wristband. At this point, the activated band can unlock appropriately provisioned devices. Nymi also provides an API for the Nymi band to communicate with custom applications; at the time this work was completed, we used the Nymi software development kit (SDK) version 2.0 and our smartphone communicated with the wristband over Bluetooth.

The MIO LINK device is not tied to a particular user and thus does not require enrollment. The device simply measures a user's heartrate when worn on the user's wrist. The heart rate signal is broadcast using Bluetooth. We paired our smartphone with the MIO LINK and polled the heart rate signal over the Bluetooth channel. Note that if multiple users were operating in close proximity, the individual MIO LINK devices would be each be paired to a unique smartphone, thus avoiding any inadvertent crosstalk.

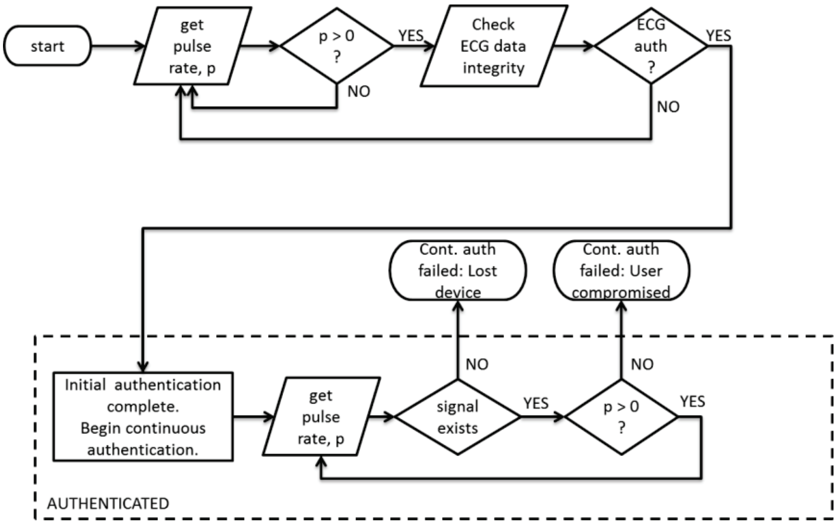
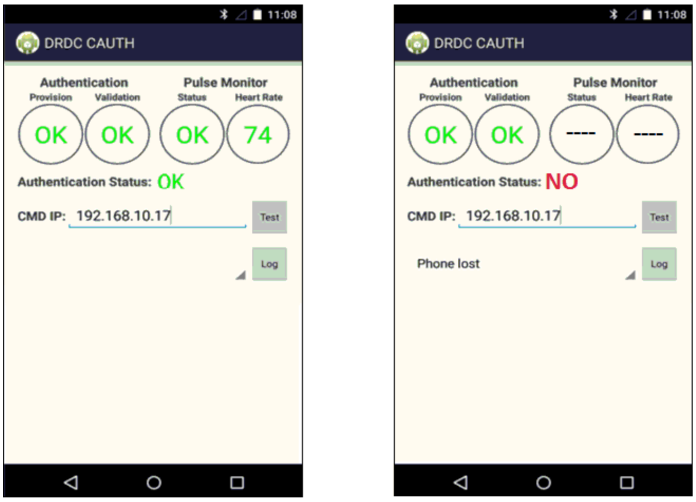


Fig. 1. Process flow of continuous authentication app. The app obtains pulse rate data from a commercial heart rate monitor and obtains ECG data integrity from a commercial ECG reader.

We created a custom smartphone app that took the inputs from both the Nymi band and MIO LINK. The process flow of the continuous authentication app is shown in Fig. 1. Initially the app ensures that a live user exists and is within range of the smartphone by checking the pulse rate from the associated MIO LINK. If the pulse rate is greater than zero, then the app will query the Nymi band. If the user had previously activated the Nymi band and has not yet removed the wrist strap, then the Nymi band will authenticate the user to the device. Note that this authentication is essentially confirming that an authenticated user put on the band at some earlier time, ran an ECG authentication (to “activate” the band) and has not yet removed it; this authentication step is not re-running the ECG, it is merely performing an integrity check that the band has not been removed.

Following the Nymi band integrity check, initial authentication is complete and the app enters a “continuity” checking phase. In this phase, the app continuously polls the MIO LINK (once per second) and confirms the presence of the MIO LINK signal. If the signal is absent for more than 3 seconds, the app concludes that the smartphone has been physically separated from the MIO LINK; the inference is that the smartphone has been lost and the app de-authenticates the user. If the signal is present but the measured pulse rate is zero, the inference is that the user has been compromised (potentially deceased) and the app de-authenticates the user. If the signal is present and the pulse is non-zero the user remains authenticated. Note that the need for the second device in addition to the Nymi band—the MIO LINK in this case—is to check for continuity of the user’s proximity and proof-of-life. The Nymi band can confirm that an authenticated user has not removed the band and thus can “unlock” a device, but it does not continually update the unlocked device with a proof-of-life signal.



Authentication Status: OK

CMD IP: 192.168.10.17

Authentication Status: NO

CMD IP: 192.168.10.17

Phone lost

(a) (b)

Fig. 2. Screenshot of continuous authentication app. The app detects the initial authentication from the ECG and the user continuity from the heart rate. In (a), initial authentication is successful and the heart rate signal is present and is non-zero. In (b), initial authentication is successful but the heart rate signal has been lost so the “Authentication Status” is set to “NO” and a message is automatically forwarded to the commander.

When a de-authentication event occurs, the app logs the event and immediately sends a message to the commander using the communication channels available in the

MANET (where it is assumed that the IP address of a commander or administrator node is provisioned ahead of time). The message to the commander indicates the ID of the smartphone that was de-authenticated along with a "reason code" for the de-authentication—either that the phone was lost or that the user was compromised.

Fig. 2 provides screenshots of the continuous authentication app. In Fig. 2(a), the app shows that the user has successfully authenticated with the Nymi band, as shown by the two green "OK" circles on the left[1]. The user's pulse signal is present (Status is "OK") and the heart rate is non-zero (it is 74 beats per minute here). Thus, this user has successfully completed initial authentication and continuity has also been maintained, leading to an overall "Authentication Status" of "OK". In Fig. 2(b), while the user has completed initial authentication, at some point the signal from the heart rate monitor was lost for more than 3 seconds, leading to an invalid status (shown as "----"). This results in an "Authentication Status" of "NO" and generates a message of "Phone lost". This message is timestamped, logged by the app, and sent to the user with the IP specified on the display (in this case the commander with IP 192.168.10.17).

3 Testing and Evaluation Results

We performed two simple experiments to evaluate the performance of our continuous authentication prototype. In the first experiment we measured the time required for the system to detect a lost device (i.e., absence of MIO LINK signal) and in the second experiment we measured the time to detect a compromised user (i.e., pulse rate of zero).

For the first experiment we conducted a series of 100 trials[2]. The procedure followed for each trial is described below, where the participants involved are a user (who wears the equipment) and an experimenter (who records the data):

1) User dons the Nymi band and MIO LINK;
2) User completes the "activation" step for the Nymi band by measuring his/her ECG reading; experimenter ensures the activation is successful (i.e., Nymi band has recognized user);
3) Experimenter ensures the MIO LINK is functioning properly (i.e., blue light on wristband is flashing approximately once per second);
4) User opens the custom continuous authentication app on the smartphone and authenticates to the smartphone (this involves pressing two buttons on the app to tell the app to begin accepting outputs from the Nymi and from the MIO LINK);

[1] Note that the two green circles in the app are labeled "provision" and "validation". These are terms and concepts used in the Nymi SDK 2.0 package. We used the "provision" and "validation" buttons to trigger the Nymi band to communicate with our app and confirm initial authentication.

[2] Note that since the trials involved testing on human subjects—including measuring and recording pulse rates and ECG readings—all testing was conducted with the approval of the DRDC Human Research Ethics Committee.

NOTE: At this point the user is authenticated to the smartphone and the app will detect a dropped phone or a compromised user.

5) User holds the smartphone, while the experimenter monitors the app for at least one minute and ensures that Authentication Status remains listed as "OK";
6) Experimenter logs a "begin test" event on the app; then the user immediately places the phone on the ground and walks away at a comfortable walking pace;
7) User continues walking, while the experimenter monitors the app until the Authentication Status changes to "NO" (at which point user can return);
8) Experimenter notes the distance travelled by the user at the instant the app changes the Authentication Status to "NO"; experimenter ensures the reason-code logged by the app for loss of authentication is due to "Phone lost".

In Fig. 3 we plotted the cumulative distribution function (cdf) of the distance travelled by the user before the lost device was detected. We note that a lost device is detected after the user has travelled a median of 13.2 meters and 95% of all lost devices are detected within 16.4 meters. The detection sensitivity depends upon the range of the BLE (Bluetooth Low Energy) signal connecting the smartphone to the MIO LINK; presumably a tighter detection range could be obtained using a lower power signal.

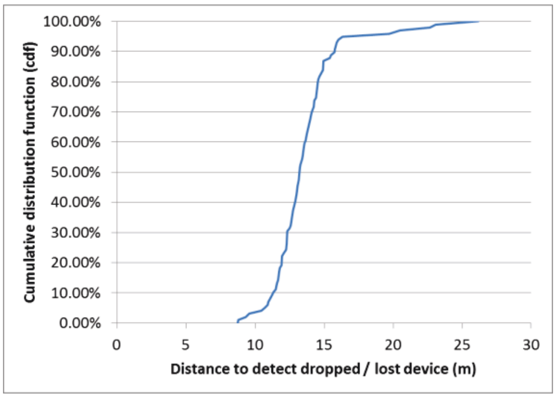


Fig. 3. Performance of continuous authentication prototype to detect a lost device showing the cdf of the distance a user has travelled before detection.

For the second experiment we conducted a series of 100 trials, where once again the participants involved were a user and an experimenter. The procedure for each trial was as follows:

NOTE: Steps 1 to 5 are identical to those followed in the first experiment.

6) Experimenter logs a "begin test" event on the app; then the user immediately removes the MIO LINK from his/her wrist;
7) The experimenter monitors the app until the Authentication Status changes to "NO";

8) Experimenter notes the time between the “begin test” log timestamp and the log timestamp at which the app changes the Authentication Status to “NO”; experimenter ensures the reason-code logged by the app for loss of authentication is due to “user health compromised”.

The cumulative distribution function (cdf) for the time to detect a user health compromise (i.e., a zero pulse rate from the MIO LINK as opposed to a loss of signal) as measured over 100 trials is shown in Fig. 4. We note that a heart rate of zero beats per minute was detected after a median time of 6.5 seconds, and 95% of all cases were detected within 9.4 seconds.

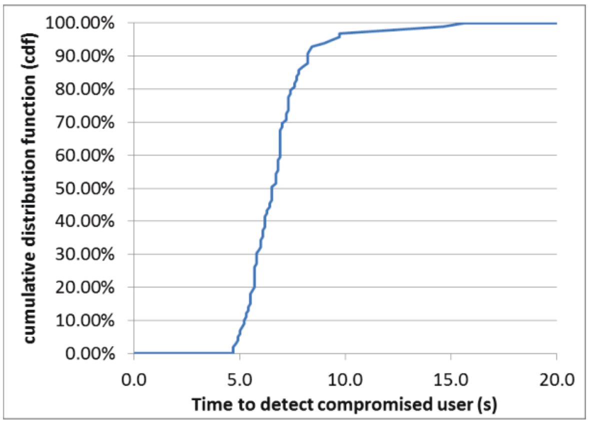


Fig. 4. Performance of continuous authentication prototype to detect user health compromise (i.e., a heart rate of zero beats per minute).

4 Discussion

In implementing the prototype app using the two commercial wristbands, it became clear that the devices were being used for two distinctly separate functions. The first, authentication, dealt with the user’s identity and was being performed by the Nymi band; the second, continuity, dealt with the ongoing validity of the user’s identity and was performed by the MIO LINK. Together these two sources of data provided an implementation of continuous authentication applicable to a military tactical network use case.

A corollary to this realization is that either function could be performed by other devices (or indeed by a single device), and that continuous authentication can be achieved by separating the “user authentication” function from the “user continuity” function. In fact, the continuity function does not need to continually validate a user’s identity—it must simply validate continuity of the presence (and life) of the user who performed the initial authentication. This is an important distinction from typical studies of continuous authentication, which generally focus on biometrics that can identify a user in an ongoing manner based on current activity that matches a stored user profile or set of features (see, for example, [9-12]). In our use case, there is no expectation that a user should ever become separated from his/her device, and there is no expectation that a device should ever "lock" once a user has authenticated. As long as the device can trace the continuity of the initial authentication, this continuity does not require an additional authentication component.

In our prototype, initial authentication is currently performed by the Nymi band, but it could be replaced by another authentication device including a fingerprint scanner, a secure token, or even a simple password. We note that the Nymi band supports password authentication as an alternative to the ECG reading, and we have found that the password authentication was generally simpler to perform. The primary advantage offered by the Nymi device is the presence of an "integrity" measure, whereby the Nymi band detects if an authenticated user has removed the band. For most commercial applications this is adequate to ensure a "continuous authentication" and to unlock a device. Unfortunately the Nymi band (in its current form) does not offer a continued proof-of-life detection such as a heart rate monitor, nor does it continue to beacon out its signal once initial authentication has taken place and the target device is unlocked—thus our use of the MIO LINK to provide "continuity". Continuity and proof-of-life could, of course, be performed by other means such as a different heart rate monitor or an alternate monitor such as body temperature, body sounds, body movement, etc.

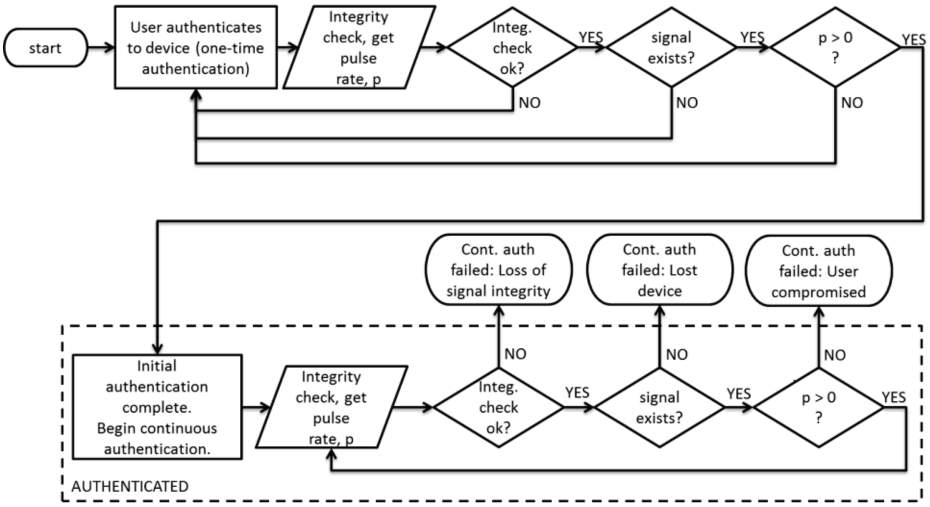

start
User authenticates to device (one-time authentication)
Integrity check, get pulse rate, p
Integ. check ok?
YES
signal exists?
YES
p > 0 ?
YES
NO
NO
NO
Cont. auth failed: Loss of signal integrity
Cont. auth failed: Lost device
Cont. auth failed: User compromised
NO
NO
NO
Initial authentication complete. Begin continuous authentication.
Integrity check, get pulse rate, p
Integ. check ok?
YES
signal exists?
YES
p > 0 ?
YES
AUTHENTICATED

Fig. 5. Recommended process flow for continuous authentication for tactical operations. Once initial (strong) authentication is complete, the primary goal of the continuous authentication system is to ensure proof-of-life and continuity of user, which can be achieved using a heart rate monitor (for proof-of-life) and a mechanical linkage (e.g., a wristband) that detects removal to ensure the integrity of the initial authentication.

In Fig. 5, we propose a process flow for continuous authentication using a single device (instead of the two devices in our prototype) that meets the requirements of our tactical military use case. A single device is mechanically linked to a user (e.g., using a wristband) and the user performs an initial authentication with the device (e.g., using a biometric, token, or password). Once initial authentication is complete, the device will maintain its "integrity" so long as the mechanical linkage is intact—that is, if the mechanical linkage is broken, the device will detect the mechanical break (as the Nymi does) and will indicate this in its communications with the smartphone. The device measures the user's pulse (or other proof-of-life, though pulse is simple and reliable) and sends the pulse signal along with an "integrity" signal at frequent periodic intervals. Three conditions would result in a de-authentication event: 1) the integrity signal is invalid, 2) the entire signal is absent, or 3) the pulse is zero. Each of these conditions would result in a different reason code for de-authentication to be presented to a commander.

The process flow in Fig. 5 is similar to the flow from Fig. 1, but includes the important addition of an integrity check with every transmission of the pulse signal. Our prototype included the integrity check only at initial authentication and then relied on the pulse signal alone to provide continuity. While the omission of the integrity check in our prototype may appear reasonable since a pulse is already a "continuous" signal, it leaves open the vulnerability of the system to an adversary that removes the heart rate monitor from our user and replaces it on his/her own wrist in the short window of time before the loss of pulse is detected (e.g., in less than the median detection time shown in Fig. 4). If an integrity check is included with each instance of the heart rate signal, the integrity check will fail in the case described above due to the loss of mechanical linkage, thus this vulnerability is averted[3].

In developing and using our prototype, we arrived at a number of other conclusions that are of interest to a military application of continuous authentication. These are summarized below:

- In a contested tactical network environment, we envision users operating as part of a MANET to communicate with the other members of their unit (e.g., Platoon, Section, Squad, etc.), where each user's node is equipped with a form of continuous authentication. Should any user's device experience a continuous authentication failure, the commander of the unit would be notified. The course of action the commander should follow at this point is not obvious. From a technical standpoint it is not difficult to lock out or disable the device. However, from an operational standpoint, this may not be the most desirable immediate course of action—perhaps the user is still there but has experienced equipment difficulties; perhaps an adversary has control of the device but it is preferable to observe what the adversary does with the device before it is disabled, etc. Ultimately, we maintain that a failure of continuous authentication that alerts the commander will empower the commander to take action; the commander could use another communication channel to determine the user's status, could request a re-authentication, could revoke the device's encryption key, could remotely zero-ize the node, or could defer the decision until more information is available, depending upon mission constraints.
- The inclusion of a "reason code" for a failure of continuous authentication is vital in order to assist a commander in determining a sensible course of

[3] Note that in our prototype we have made the tacit assumption that the BLE connection between the wristbands and the smartphone is secure. To ensure the security of this connection is beyond the scope of this paper.

action in response. For instance, if the reason for failure is deemed a "lost device", it might be reasonable to remotely lock the device, but at the same time allow the device to continue broadcasting situational awareness messages in order to more easily locate and recover the device. If the reason for failure is a "user compromise", the commander may wish to direct immediate effort (including medical expertise) to the last known location of the user.

- For nodes that are part of a MANET, it is possible that certain nodes will be disconnected from the commander at any given time. Should a node fail continuous authentication while disconnected from the commander, the commander may miss the notification of the failure. We suggest that it may be desirable for nodes to periodically transmit continuous authentication status information to the commander as part of their standard situational awareness updates. In this fashion, the commander will be notified of the failure as soon as the node returns in range and the commander receives a situational awareness update.
- In our prototype, the two wristbands communicated with the smartphone using Bluetooth Low Energy. Relying on a wireless connection (commercial or otherwise) for continuous user authentication is problematic as it may be vulnerable to jamming and other simple denial of service techniques. In addition to simple jamming, BLE (or other standard protocols) may be vulnerable to spoofing at the protocol level. A wired connection to other body sensors is more robust, however this presents problems as well since additional wiring to mechanical linkages and body sensors may be cumbersome. The choice ultimately depends upon envisioned use cases and adversarial capabilities.

5 Conclusion

In this paper, we presented a prototype implementation of a continuous authentication system for a military tactical network use case in which two commercial biometric wristbands were tethered to a smartphone in a MANET; the prototype system detects if a user loses the smartphone or becomes compromised. For our use case, we observed that continuous authentication can be achieved by a device that monitors the continued presence of the user following an initial strong authentication. It is not necessary for the continued presence to validate the identity of the user, but merely to confirm the continuity of the user from initial login. We recommend the use of an authentication device that contains a mechanical linkage (e.g., a wristband) that can perform initial authentication and also detect the continued presence of a user (e.g., through a heart rate monitor). With such a device, any loss of continuity or integrity—either through a loss of heart rate signal or a loss of mechanical linkage—would result in a de-authentication event. Developing or implementing such a device is feasible today using existing commercial products and could increase the usability and security of mobile devices for tactical applications.

References

1. Directorate of Land Concepts and Design, Department of National Defence, Government of Canada, “Land Operations 2021: Adaptive Dispersed Operations, the Force Employment Concept for Canada’s Army of Tomorrow”, 2007.
2. Canadian Army Land Warfare Centre, Department of National Defence, Government of Canada, “No Man’s Land: Tech Considerations for Canada’s Future Army”, 2012.
3. David S. Alberts, John J. Garstka, Frederick P. Stein, *Network Centric Warfare*, CCRP Publication Series, August 1999, available at http://dodccrp.org/files/Alberts_NCW.pdf.
4. David S. Alberts, Richard E. Hayes, *Power to the Edge*, CCRP Publication Series, June 2003, available at http://www.dodccrp.org/files/Alberts_Power.pdf.
5. Fabian Monrose, Aviel D. Rubin, “Keystroke Dynamics as a Biometric for Authentication”, in *Future Generation Computer Systems* vol. 16, pp. 351-359, 2000.
6. M. S. Hossain, Kiran S. Balagani, V. V. Phoha, “New Impostor Score Based Rejection Methods for Continuous Keystroke Verification with Weak Templates” in *Proc. of 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems*, September 2012.
7. Joseph Roth, Xiaoming Liu, Dimitris Metaxas, “On Continuous User Authentication via Typing Behavior”, *IEEE Transactions on Image Processing*, vol. 23, no. 10, October 2014.
8. Ahmed Awad E. Ahmed, Issa Traore, “A New Biometric Technology Based on Mouse Dynamics”, *IEEE Transactions on Dependable and Secure Computing*, July-September 2007.
9. Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, B. Carbunar, Yifei Jiang, N. Nguyen, “Continuous Mobile Authentication Using Touchscreen Gestures”, in *Proc. of 2012 IEEE Conference on Technologies for Homeland Security*, November 2012.
10. Arun Balaji Buduru, Stephen S. Yau, “An Effective Approach to Continuous User Authentication for Touch Screen Smart Devices”, in *Proc. of IEEE International Conference on Software Quality, Reliability and Security (QRS)*, August 2015.
11. Xi Zhao, Tao Feng, Lei Xu, Weidong Shi, “Mobile User Identity Sensing Using the Motion Sensor”, in *Proc. of SPIE DSS*, Baltimore MD, May 2014.
12. David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, Anil K. Jain, “Continuous Authentication of Mobile User: Fusion of Face Image and Inertial Measurement Unit Data”, in *Proc. of 2015 IEEE International Conference on Biometrics (ICB)*, May 2015.
13. L. Biel, O. Pettersson, L. Philipson and P. Wide, “ECG Analysis: A New Approach in Human Identification,” *IEEE Transaction on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808-812, 2001.
14. S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold and B. K. Wiederhold, “ECG to Identify Individuals,” *Pattern Recognition*, vol. 38, no. 1, pp. 133-142, 2005.
15. Y. Wang, F. Agrafioti, D. Hatzinakos and K. N. Plataniotis, “Analysis of Human Electrocardiogram for Biometric Recognition,” *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1-11, 2008.
16. Y. N. Singh and P. Gupta, “Biometric Method for Human Identification Using Electrocardiogram,” in *Proc. of the 3rd IAPR/IEEE International Conference on Biometrics, ICB 2009*, LNCS, Springer-Verlag, Berlin, vol. 5558, pp. 1270-1279, 2009.
17. Nymi corporate website: www.nymi.com, accessed 16-May-2016.
18. MIO LINK brochure website: http://www.mioglobal.com/Mio-Link-heart-rate-wristband/Product.aspx, accessed 16-May-2016.